

**UNIVERSIDAD CAMILO JOSÉ CELA**

**ESCUELA INTERNACIONAL DE DOCTORADO**

**Programa de Doctorado en Ciencias Jurídicas y Económicas**

**UNIVERSO *FINTECH*: DE LA EVOLUCIÓN A LA DISRUPCIÓN DE LA  
TECNOLOGÍA EN FINANZAS. MARCOS DE SUPERVISIÓN Y  
REGULACIÓN**

**TESIS DOCTORAL**

**LUCÍA SUÁREZ BARCIA**

Bajo la dirección de la

**Dra. D<sup>a</sup>. Ana Felicitas Muñoz Pérez**

Tutor

**Francisco Santamaría Ramos**

**Madrid, 2023**



## **AGRADECIMIENTOS**



## **AGRADECIMIENTOS**

La investigación y redacción de esta tesis lleva a sus espaldas una larga lista de personas sin las que este trabajo no hubiera sido posible. En mayor o menor medida, todos ellos me han apoyado en aspectos personales y técnicos.

Quiero agradecer a mi directora de tesis y mi tutor, por su constante seguimiento, positivismo y buen hacer. Quisiera agradecer a mi familia, en especial a mi marido y a mis hijos que han intentado comprender y aportar en este mundo tan complicado de entender. No puedo dejar de reconocer la paciencia de mis seres queridos (los que están y los que ya no están con nosotros), así como a mis conocidos por haber facilitado siempre que me pudiera enfocar en la investigación de un tema tan apasionante como complejo, sin perder nunca los objetivos marcados. Reconozco que soy afortunada de estar rodeada de grandes profesionales de los que aprendo cada día.

El viaje ha sido una experiencia enriquecedora, no sólo gracias a ellos, sino también a las instituciones que me han acogido en mi labor investigadora (Universidad Camilo José Cela, IE University y Karlsruhe Institute of Technology).

Finalmente, no tengo sino palabras de gratitud a todos aquellos que han leído algún borrador (total o parcial) de esta tesis, aportando puntos de mejora o nuevos derroteros por los que investigar.



## ÍNDICE





# UNIVERSO *FINTECH*: DE LA EVOLUCIÓN A LA DISRUPCIÓN DE LA TECNOLOGÍA EN FINANZAS. MARCOS DE SUPERVISIÓN Y REGULACIÓN

## ÍNDICE

AGRADECIMIENTOS .....	3
ÍNDICE .....	7
ABREVIATURAS .....	17

## INTRODUCCIÓN

I. CONTEXTO, RELEVANCIA Y OBJETIVOS.....	31
II. HIPÓTESIS DE INVESTIGACIÓN .....	35
III. METODOLOGÍA.....	36
IV. ESTRUCTURA .....	38

## *PRIMERA PARTE: EL FENÓMENO FINTECH*

### *CAPÍTULO I. CONSIDERACIONES PREVIAS*

I. DEFINICIÓN .....	47
II. LA INNOVACIÓN TECNOLÓGICA: EVOLUCIÓN O CAMBIO DE PARADIGMA.....	52
1. Instituciones financieras establecidas ( <i>incumbents</i> ): argumento evolutivo ...	52
2. Emprendedores en el sector ( <i>start-ups</i> ): argumento de disrupción .....	53
3. Entidades tecnológicas en finanzas ( <i>TechFin</i> ): la disrupción de las masas..	54
4. Perspectiva del público: consumidores e inversores no institucionales .....	56
5. <i>FinTech</i> desde la perspectiva de los reguladores y supervisores: afrontar el fenómeno.....	57
III. PROBLEMÁTICA DE LAS FINANZAS TRADICIONALES Y <i>FINTECH</i> COMO SU RESPUESTA.....	57
1. Control centralizado.....	58
2. Limitación de acceso .....	58
3. Ineficiencia .....	59
4. Falta de interoperabilidad.....	60
5. Opacidad.....	61

## ***CAPÍTULO II. ANTECEDENTES: FINTECH 1.0 Y FINTECH 2.0***

<b>I. INTRODUCCIÓN .....</b>	<b>63</b>
<b>II. FINTECH 1.0: EL HARDWARE Y LA INTERCONEXIÓN DE PAÍSES. 63</b>	
<b>III. FINTECH 2.0: LOS SERVICIOS DE PAGOS Y SUS</b>	
<b>INFRAESTRUCTURAS.....</b>	<b>65</b>
<b>IV. ENFOQUES DE SUPERVISIÓN.....</b>	<b>68</b>

## ***CAPÍTULO III. HACIA EL CAMBIO DE PARADIGMA: FINTECH 3.0-3.5***

<b>I. INTRODUCCIÓN .....</b>	<b>71</b>
1. <i>Diferenciación entre FinTech 3.0 y FinTech 3.5.....</i>	72
2. <i>Los agentes .....</i>	74
2.1 <i>FinTech start-up .....</i>	75
2.2 <i>TechFin (BigTechs) .....</i>	76
2.3 <i>Entidades financieras (incumbents) .....</i>	79
2.4 <i>Comparativa.....</i>	81
<b>II. FINTECH 3.0: LA BANCA ABIERTA EN EUROPA .....</b>	<b>82</b>
1. <i>Planteamiento .....</i>	82
1.1 <i>Revolución en las entidades intervinientes .....</i>	84
1.2 <i>Revolución en las infraestructuras .....</i>	84
2. <i>Aproximación a las PayTech .....</i>	85
3. <i>Los sujetos. Criterios de clasificación de las PayTech .....</i>	87
3.1 <i>Taxonomía en función del tipo de licencias .....</i>	87
3.2 <i>Según su actividad .....</i>	89
5. <i>Recapitulación y observaciones sobre entidades intervinientes.....</i>	97
6. <i>FinTech 3.0 en infraestructuras .....</i>	98
6.1 <i>Planteamientos iniciales.....</i>	98
6.2 <i>Acciones tomadas por los organismos internacionales.....</i>	99
6.3 <i>Panorama de los pagos internacionales en la actualidad .....</i>	100
6.4 <i>Nociones previas: clasificaciones de los pagos .....</i>	101
6.5 <i>Problemática de los sistemas de pagos .....</i>	103
6.6 <i>Innovación tecnológica como solución.....</i>	107
6.7 <i>Implicaciones regulatorias y de gobernanza de estas propuestas ...</i>	114
6.8 <i>Recapitulación en lo afectante a infraestructuras de pago .....</i>	117
<b>III. FINTECH 3.5: LAS FINANZAS ABIERTAS .....</b>	<b>117</b>
1. <i>Introducción.....</i>	117

1.1 De la banca abierta a las finanzas abiertas.....	119
1.2 Ventajas para los usuarios: autosoberanía de datos y mejora de la gestión.....	121
1.3 Riesgos.....	122
1.4 Protagonismo de los países emergentes en FinTech 3.5.....	123
2. <i>Los sujetos. Las BigTech</i> .....	125
2.1 El peso de los gigantes BigTech en las finanzas: el fenómeno TechFin .....	125
3. <i>Las actividades. Análisis de la transformación FinTech 3.5 desde la perspectiva de sus productos y servicios</i> .....	136
4. <i>Transformación vertical</i> .....	138
4.1 Servicios de pasivo y asociados: billeteras, entidades emisoras de dinero electrónico e innovaciones en pagos.....	138
4.2 Servicios de activo .....	140
4.3 Productos de inversión.....	158
4.4 Otros servicios: InsurTech .....	165
4.5 RegTech y SupTech.....	169
5. <i>Transformación horizontal: fraccionamientos de la cadena de valor. Proliferación de los negocios “as a Service”</i> .....	176
5.1 Descripción de las actividades .....	176
5.2 Situación actual. PSD II como habilitador.....	179
5.4 Las API como elemento clave de estos modelos .....	180
5.5 Banking as a Service .....	183
5.6 FinTech as a Service .....	186
5.7 Oportunidades .....	187
5.8 Problemáticas que plantean.....	188
5.9 Propuesta de criterios mínimos legales y regulatorias.....	193
<b>IV. FINTECH 3.0 y 3.5: ¿DESINTERMEDIACIÓN O REINTERMEDIACIÓN?</b> .....	<b>195</b>
<b>V. RECAPITULACIÓN. ANÁLISIS DE MARCOS REGULATORIOS Y DE SUPERVISIÓN FINTECH 3.5</b> .....	<b>196</b>

## ***CAPÍTULO IV. FINTECH 4.0: LA DISRUPCIÓN***

<b>I. INTRODUCCIÓN: CONTEXTO GENERAL</b> .....	<b>199</b>
<b>II. ELEMENTOS DE CARACTERIZACIÓN</b> .....	<b>200</b>
1. <i>Blockchain como puerta de acceso</i> .....	200
2. <i>Los contratos inteligentes como nuevo sistema de establecimiento de reglas</i> .....	204
3. <i>Los tokens o fichas</i> .....	207

4. Aplicaciones descentralizadas y organizaciones autónomas descentralizadas .....	208
<b>III. FINANZAS DESCENTRALIZADAS (DEFI) .....</b>	<b>216</b>
1. Finanzas descentralizadas (DeFi) y su propósito .....	216
2. Evolución de CeFi a DeFi y el cambio en la figura del tercero de confianza .....	219
3. Niveles de descentralización.....	219
4. Las nuevas contrapartes .....	221
5. Infraestructura.....	224
<b>IV. CRIPTOMONEDAS O CRIPTODIVISAS.....</b>	<b>228</b>
1. Activos digitales: criptoactivos y criptomonedas .....	228
2. Criptomonedas de emisión privada .....	229
2.1 Bitcoin.....	229
2.2 Ether.....	231
2.3 Stablecoins o criptomonedas estables.....	232
3. Criptoactivos de emisión pública: monedas digitales de bancos centrales .	240
3.1 Introducción .....	240
3.2 Estado de la cuestión.....	241
3.3 CBDC: concepto, tipos y finalidad .....	242
3.4 Casos de uso, ventajas y riesgos de las CBDC .....	243
3.5 ¿Por qué CBDC ahora? Geopolítica, finanzas y criptoactivos .....	245
3.6 Retos jurídico-económicos para los bancos centrales.....	247
3.7 Categorías de controversia: non fungible token (NFT o token no fungible).....	248
4. Análisis crítico de los elementos de riesgo.....	256
4.1 Gobernanza .....	257
4.2 Conflictos de interés .....	259
4.3 Crimen financiero .....	260
4.4 Protección de datos, transparencia y protección al consumidor .....	264
4.5 Gestión de riesgos operacionales y ciberseguridad .....	266
<b>V. MODELOS FINANCIEROS DESCENTRALIZADOS .....</b>	<b>267</b>
1. Productos de pasivo: las billeteras y los pagos descentralizados.....	268
2. Productos de activo: financiación descentralizada.....	270
2.1 Crédito.....	270
2.2 Initial Loan Procurements (ILP) .....	273
2.3 Crowdfunding descentralizado .....	273
3. La transformación de los servicios de inversión .....	274
3.1 Métodos de emisión cripto.....	274
3.2 Exchanges descentralizados (casas de cambio) y Automated Money Market Makers (mercados de dinero automatizados).....	279

3.3 Gestión de carteras o gestión de activos .....	284
3.4 Agregadores de rendimiento .....	285
3.5 Derivados y predicción de eventos .....	286
4. Otros servicios .....	287
4.1 Servicios fundacionales: custodia de criptoactivos.....	287
4.2 Servicios adyacentes .....	292
5. Nuevos servicios nativos del mundo cripto: oráculos .....	295
5.1 Concepto y tipos .....	295
5.2 Casos de uso.....	297
5.3 Problemáticas que plantean.....	298
<b>VI. EL ROL DE LA BANCA INSTITUCIONAL EN FINTECH 4.0 .....</b>	<b>299</b>
<b>VII. RETOS: ENFOQUE BASADO EN RIESGOS Y</b>	
<b>PROPORCIONALIDAD APLICADOS A POLÍTICAS REGULATORIAS</b>	<b>302</b>
<b>VIII. METAVERSOS. LA NECESIDAD DE MARCOS NORMATIVOS</b>	
<b>PROPIOS .....</b>	<b>304</b>
<b>IX. PRINCIPALES MENSAJES .....</b>	<b>306</b>

## *SEGUNDA PARTE. RETOS DE SUPERVISIÓN Y REGULACIÓN*

### *CAPÍTULO V. SUPERVISIÓN FINTECH: LA TEORÍA DEL DESFASE*

#### *SUPERVISOR*

<b>I. LOS MECANISMOS TRADICIONALES DE SUPERVISIÓN.....</b>	<b>313</b>
1. Planteamiento .....	313
2. La gobernanza de la supervisión financiera .....	313
3. Arquitecturas de supervisión .....	315
3.1 Comités de coordinación a nivel europeo: el comité conjunto de autoridades de supervisión europeas.....	315
3.2. Mecanismo Único de Supervisión .....	317
<b>II. LA TEORÍA DEL DESFASE SUPERVISOR.....</b>	<b>322</b>
1. La problemática.....	322
2. Evidencia del desfase: el caso de la regulación del “travel rule” .....	329
<b>III. SANDBOX REGULATORIO. CONTROVERSIA DE POLÍTICA</b>	
<b>JURÍDICA.....</b>	<b>331</b>

**CAPÍTULO VI. REGULAR FINTECH: ESTADO ACTUAL Y PROPUESTA A  
FUTURO**

<b>I. PLANTEAMIENTO.....</b>	<b>335</b>
1. Modelos de regulación FinTech y potenciales mejoras .....	335
2. Tipologías de regulación bancaria en general.....	335
3. Flujos de producción normativa.....	337
4. Procesos operacionales de desarrollos regulatorios .....	338
<b>II. OPCIONES DE POLÍTICA JURÍDICA .....</b>	<b>340</b>
<b>III. LA APLICACIÓN DE LA ANALOGÍA EN FINTECH .....</b>	<b>344</b>
1. Planteamiento .....	344
2. Analogía en FinTech: misma actividad, mismos riesgos, mismas reglas ....	350
2.1 Juicio fáctico de la misma actividad .....	351
2.2 Juicio fáctico de mismo riesgo.....	353
2.3 Juicio lógico de misma norma .....	355
3. En concreto, la posible regulación marco de modelos FinTech 4.0 .....	357
2.1 Planteamiento de posibles nuevos regímenes de licencias .....	359
2.2 Avance de potenciales modelos de regulación supervisora.....	360
2.3 Ámbito subjetivo, los potenciales nuevos sujetos obligados .....	362
3. Recapitulación .....	364

**CHAPTER VII. CRITICAL ASSESSMENT OF SPECIFIC REGULATORY  
INITIATIVES**

<b>I. GLOBAL INITIATIVES .....</b>	<b>367</b>
<b>II. EUROPEAN FRAMEWORK .....</b>	<b>370</b>
1. FinTech Action Plan of 2018 .....	371
2. Digital Finance Strategy for the EU (2020) .....	373
<b>III. AD-HOC MODELS. MARKETS IN CRYPTO ASSETS .....</b>	<b>375</b>
1. Objective .....	375
2. Main elements of the regulation .....	376
2.1 Subject matter, scope, and definitions .....	377
2.2 Crypto assets taxonomy in MiCA.....	382
2.3 Crypto assets service providers (CASP) .....	388
2.3 Market abuse .....	391
3. Observations .....	392
3.1 General critics and aspects for improvement.....	392

3.2	Technical questions and observations.....	395
4.	<i>Main outcomes: MiCA II before even publishing MiCA I</i> .....	398
<b>IV.</b>	<b>AD-HOC MODEL OF DLT PILOT REGIME .....</b>	<b>399</b>
1.	<i>Objective</i> .....	400
2.	<i>Main elements</i> .....	401
3.	<i>Advantages</i> .....	406
4.	<i>Observations</i> .....	408
4.1	Operations and Settlement via distributed ledger technology .....	408
4.2	Technical.....	409
5.	<i>Main outcomes</i> .....	411
<b>V.</b>	<b>AD-HOC MODEL OF OPERATIONAL RESILIENCE IN EUROPE:</b>	
<b>DORA</b>	<b>412</b>	
1.	<i>Objective</i> .....	412
2.	<i>Main elements</i> .....	413
3.	<i>Advantages</i> .....	417
4.	<i>Observations</i> .....	418
4.1	General.....	418
4.2	Technical.....	420
5.	<i>Main outcomes</i> .....	429
<b>VI.</b>	<b>AD-HOC TRANSVERSAL MODELS: DIGITAL MARKETS ACT (DMA)</b>	
<b>AND DIGITAL SERVICES ACT (DSA)</b>	<b>.....</b>	<b>430</b>
<b>VII.</b>	<b>REVIEW OF EXISTING FRAMEWORKS .....</b>	<b>435</b>
1.	<i>The digital identity: eIDAS 2</i> .....	435
1.1	The basis line: eIDAS 1 effectiveness .....	436
1.2	eIDAS 2 overview and its impact on the financial industry .....	438
2.	<i>FinTech 3.5 in Europe: PSD II towards PSD III?</i> .....	442
2.1	PSD II overview.....	442
2.2	PayTech regulatory framework proposal.....	443
2.3	Towards PSD II or something different?.....	444
2.4	The need for a dialogue between MiCA and the Payment Services Directive.....	449

## **CHAPTER VIII. CONCLUSION**

### **ANEXOS**

<b>ANEXO I. GLOSARIO.....</b>	<b>463</b>
-------------------------------	------------

<b>ANEXO II. ANÁLISIS DE DEFINICIONES <i>FINTECH</i>.....</b>	<b>467</b>
<b>ANEXO III. ETAPAS <i>FINTECH</i> Y SUS CARACTERÍSTICAS .....</b>	<b>477</b>
<b>ANEXO IV. PUBLICACIONES .....</b>	<b>481</b>

***ÍNDICES***

<b>ÍNDICE DE TABLAS .....</b>	<b>485</b>
<b>ÍNDICE DE FIGURAS .....</b>	<b>487</b>
<b><i>REFERENCIAS</i> .....</b>	<b>489</b>



## **ABREVIATURAS**



## ABREVIATURAS

Abreviatura	Significado
AEB	Asociación Española de Banca.
AEFI	Asociación Española de <i>FinTech</i> e <i>InsurTech</i> .
AFME	<i>Association for Financial Markets in Europe</i> . Asociación Europea para los Mercados de Capitales.
AIFMD	<i>Alternative Investment Fund Managers Directive</i> . Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) N.º 1060/2009 y (UE) N.º 1095/2010 Texto pertinente a efectos del EEE.
AISP	<i>Account information service provider</i> . Proveedores de servicios de agregación de información sobre cuentas.
AML/CFT	<i>Anti-money Laundering and Counter Terrorist Financing</i> . Prevención de blanqueo de capitales y de financiación del terrorismo.
AMM	<i>Automated market makers</i> . Creador automático de mercado.
API	<i>Application Programming Interface</i> . Interfaz de programación de aplicaciones.
ART	<i>Asset Reference Tokens</i> . Fichas referenciadas a activos.
ASCOM	Asociación Española de Compliance.
ASPSP	<i>Account Servicing Payment Service Providers</i> . Proveedores de servicios de pago de servicios de cuenta.
ATM	<i>Automated teller machine</i> . Cajero automático.
AWS	Amazon Web Services.
B2B	<i>Business to business</i> . De negocio a negocio.
B2C	<i>Business to consumer</i> . De negocio a consumidor.
BaaS	<i>Banking as a Service</i> . Banca como servicio.
BACS	<i>Bankers Automated Clearing Service</i> . Servicio de Compensación Automatizado de Banqueros.
BATX	Baidu, Alibaba, Tencent y Xiaomi.
BIS	<i>Bank of International Settlements</i> . Banco de Pagos Internacionales.
BTC	Bitcoin.
C2B	<i>Consumer to business</i> . De consumidores a negocio.
CASP o VASP	<i>Cryptoasset service provider</i> (Unión Europea) o <i>Virtual Asset Service Provider</i> (otras regiones). Proveedor de servicios de criptoactivos o proveedor de servicios de activos virtuales.

<b>Abreviatura</b>	<b>Significado</b>
CBDC	<i>Central Bank Digital Currency</i> . Moneda digital de banco central.
CeDeFi	<i>Centralized Decentralized Finance</i> . Descentralización centralizada en finanzas.
CeFi o TradFi	<i>Centralized or traditional finance</i> . Finanzas centralizadas o tradicionales.
CFSB	<i>Community Federal Savings Bank (USA)</i> . Banco Comunitario de Ahorro Federal Estadounidense.
CHIPS	<i>Clearing House Interbanks Payment System</i> . Sistema de Pagos Interbancarios de la Cámara de Compensación Estadounidense.
CIRBE	Central de Información de Riesgos del Banco de España.
CMA	<i>International Capital Markets Association</i> . Asociación internacional de mercados de capitales.
CNMC	Comisión Nacional del Mercado y la Competencia.
CNMV	Comisión Nacional del Mercado de Valores.
CPMI	<i>Committee on Payments and Market Infrastructures</i> . Comité de Pagos e Infraestructuras del Banco de Pagos Internacionales ( <i>Bank of International Settlements</i> o BIS).
CRD V	Directiva (UE) 2019/878 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 por la que se modifica la Directiva 2013/36/UE en lo que respecta a los entes exentos, las sociedades financieras de cartera, las sociedades financieras mixtas de cartera, las remuneraciones, las medidas y las facultades de supervisión y las medidas de conservación del capital Reglamento (UE) 2019/876 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 por el que se modifica el Reglamento (UE) n.º 575/2013 en lo que se refiere a la ratio de apalancamiento, la ratio de financiación estable neta, los requisitos de fondos propios y pasivos admisibles, el riesgo de crédito de contraparte, el riesgo de mercado, las exposiciones a entidades de contrapartida central, las exposiciones a organismos de inversión colectiva, las grandes exposiciones y los requisitos de presentación y divulgación de información, y el Reglamento (UE) n.º 648/2012
CRR 2	
CRS	<i>Common Reporting Standards</i> . Estándar Común de Reporte.
CSD	<i>Central Securities Depository</i> . Depósito central de valores.
CSRD	Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la mejora de la liquidación de valores en la Unión Europea y los depositarios centrales de valores y por el que se

<b>Abreviatura</b>	<b>Significado</b>
	modifican las Directivas 98/26/CE y 2014/65/UE y el Reglamento (UE) n.º 236/2012
CSSF	<i>Commission de Surveillance du Secteur Financier</i> . Comisión de Supervisión del Sector Financiero (Luxemburgo).
DAO	<i>Decentralized Autonomous Organization</i> . Organización Autónoma Descentralizada.
DApp	<i>Decentralized application</i> . Aplicación descentralizada.
DeFi	<i>Decentralized Finance</i> . Finanzas descentralizadas.
DEX	<i>Decentralized exchange</i> . Plataforma de intercambio de activos digitales descentralizada.
Diem (ex-Libra)	Proyecto fallido de <i>stablecoin</i> global, sistémica o significativa liderado por Facebook (actualmente Meta).
DLT	<i>Distributed Ledger Technology</i> . Tecnología de Registros Distribuidos.
DLT MTF	<i>Distributed ledger technology multilateral trading facilities</i> . Sistema multilateral de negociación basado en la tecnología de registros distribuidos o «SMN basado en la TRD»
DLT SS	<i>Distributed ledger technology settlement systems</i> . Sistema de liquidación basado en la tecnología de registros distribuidos o «SL basado en la TRD»
DLT TSS	<i>Distributed ledger technology trading and settlement systems</i> . Sistema de negociación y liquidación basado en la tecnología de registros distribuidos o «SNL basado en la TRD».
DMA	<i>Digital Markets Act</i> . Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). <i>Digital Operational Resilience Act</i> . Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/101.
DORA	
DPoS	<i>Delegated Proof of Stake</i> . Prueba de participación delegada.
DSA	<i>Digital Services Act</i> . Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

<b>Abreviatura</b>	<b>Significado</b>
DSP	Directiva de Servicios de Pago. Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) N.º 1093/2010 y se deroga la Directiva 2007/64/CE.
DYCO	<i>Dynamic Coin Offering</i> . Oferta dinámica de criptomonedas.
EBA o ABE	<i>European Banking Authority</i> . Autoridad Bancaria Europea.
EBF	<i>European Banking Federation</i> . Federación de Bancos Europeos.
EBSI	<i>European Blockchain Services Infrastructure</i> . Infraestructura de Servicios Blockchain Europeos
EC o CE	<i>European Commission</i> . Comisión Europea
ECB o BCE	<i>European Central Bank</i> . Banco Central Europeo
ECC	<i>Electronic Communications Convention of United Nations</i> . Acuerdo de comunicaciones electrónicas en los contratos internacionales.
eIDAS 1	Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
eIDAS 2	Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. COM/2021/281 final.
EIOPA	<i>European Insurance and Occupational Pensions Authority</i> . Autoridad Europea de Seguros y Pensiones de Jubilación.
EMI o EDE	<i>Electronic Money Institution</i> . Entidad de Dinero Electrónico.
EMT	<i>E-money Tokens</i> . Fichas referenciadas a dinero electrónico o fichas de dinero electrónico.
ENISA	<i>European Union Agency of Cybersecurity</i> . Agencia Europea de Ciberseguridad.
EPIF	<i>European Payment Institutions Federation</i> . Federación Europea de Instituciones de Pago.
ERC	<i>Ethereum Requests for Comments</i> . Solicitud de Comentarios para Ethereum (modelo de generación de <i>tokens</i> ).
ESFS	<i>European System of Financial Supervision</i> . Sistema Europeo de Supervisión Financiera.

<b>Abreviatura</b>	<b>Significado</b>
ESG	<i>Environmental, Social and Governance.</i> Medioambiente, Social y Gobernanza.
ESMA	<i>European Securities and Markets Authority.</i> Autoridad Europea de Valores y Mercados.
ESRB	<i>European Systemic Risk Board.</i> Junta Europea de Riesgo Sistémico.
ETH	Ethereum.
EU o UE	<i>European Union.</i> Unión Europea.
FaaS	<i>FinTech as a Service.</i> FinTech como servicio.
FATCA	<i>Foreign Account Tax Compliance Act.</i> Acta de Cumplimiento Fiscal de Cuentas en el Extranjero (Norma estadounidense de alcance extraterritorial).
FATF o GAFI	<i>Financial Action Task Force.</i> Grupo de Acción Financiera Internacional.
FCA o UK FCA	<i>Financial Conduct Authority.</i> Regulador de Reino Unido.
FSB	<i>Financial Stability Board</i>
GAFA	Google, Amazon, Facebook y Apple
GDPR	Reglamento General de Protección de Datos. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)
GSIFI	<i>Global Systemically Financial Institutions.</i> Instituciones Financieras Globalmente Sistémicas.
G-SIIS	<i>Global Systemically Important Insurers.</i> Instituciones Aseguradoras Globalmente Sistémicas.
GUI	<i>Graphic user interface.</i> Interfaces gráficas de usuario.
HQLA	<i>High quality liquidity assets.</i> Activos de alta calidad y liquidez.
IAASB	<i>International Audit and Assurance Standards Board.</i> Junta de Normas Internacionales de Auditoría y Aseguramiento.
ICO	<i>Initial Coin Offering.</i> Oferta inicial de criptomonedas.
ICT o TIC	<i>Information and Communication Technologies.</i> Tecnologías de la Información y Comunicación.
IDO	<i>Initial Dex Offering.</i> Oferta inicial descentralizada de criptomonedas.
IEC	<i>International Electrotechnical Commission.</i> Comisión Electrotécnica Internacional.

<b>Abreviatura</b>	<b>Significado</b>
IEO	<i>Initial Exchange Offering</i> . Oferta inicial de criptomonedas via plataformas de intercambio centralizadas.
IFO	<i>Initial Farm Offering</i> . Oferta inicial de granja u oferta inicial de fichas nuevas a precios especiales de venta anticipada antes de que se abran al público.
ILM	<i>Initial Loan Procurement</i> . Adquisición de préstamo inicial de <i>tokens</i> .
IMF	<i>International Monetary Fund</i> . Fondo Monetario Internacional.
IOSCO	<i>International Organization of Securities Commissions</i> . Organización Internacional de Comisiones de Valores.
IoT	<i>Internet of the things</i> . Internet de las cosas.
IPSI	<i>International payment settlement infrastructure</i> . Infraestructura de pagos multilaterales ( <i>Bundesbank</i> ).
ISIN	<i>International Securities Identification Number</i> . Número de identificación de valores internacionales.
ISO	<i>International Organization for Standardization</i> . Organización Internacional de Normalización.
ITSA	<i>International Token Standardization Association</i> . Asociación Internacional de Estandarización de <i>Tokens</i> .
JCESA	<i>Joint Committee of the European Supervisory Authorities</i> . Comité conjunto de autoridades de supervisión europeas
KYC	<i>Know Your Customer</i> . Conoce a tu cliente.
KYT	<i>Know Your Transaction</i> . Conoce a tu transacción.
LEI	<i>Legal entity identifier</i> . Identidad de persona jurídica.
LFPE	Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial.
LLC	<i>Limited liability company</i> . Sociedad de responsabilidad limitada.
LMV	Ley del Mercado de Valores. Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores.
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
M2M	<i>Machine to machine</i> . Máquina a máquina.
MAD	Directiva 2014/57/UE del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre las sanciones penales aplicables al abuso de mercado (Directiva sobre abuso de mercado).



<b>Abreviatura</b>	<b>Significado</b>
MAR	Reglamento (UE) n° 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión.
MENA	<i>Middle East and North Asia</i> . Oriente Medio y Norte de Asia.
MiCA o MiCA	Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937.
MiFID II	Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (refundición) (Texto pertinente a efectos del EEE).
MiFIR	Reglamento (UE) N.° 600/2014 del Parlamento Europeo y del Consejo del 15 de mayo de 2014 relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) no 648/2012 (Texto pertinente a efectos del EEE).
MLETR	<i>Model Law on Electronic Transferable Records</i> . Ley Modelo sobre Documentos Transmisibles Electrónicos de las Naciones Unidas.
MUS	Mecanismo Único de Supervisión.
NASDAQ	<i>National Association of Securities Dealers Automated Quotations</i>
NFC	<i>Near Field Communication</i> . Comunicación de campo cercano.
NFT	<i>Non fungible token</i> . Ficha o <i>token</i> no fungible.
NIS 1	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
NIS 2	Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n° 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
NIST	<i>National Institute of Standards and Technology</i> . Instituto Nacional de Normas y Tecnología.

<b>Abreviatura</b>	<b>Significado</b>
NLF	<i>Natural language processing</i> . Procesamiento natural del lenguaje
OCR	<i>Optical Character Recognition</i> . Reconocimiento de caracteres ópticos.
OECD u OCDE	Organización para la Cooperación y el Desarrollo Económicos.
OICV	Organización Internacional de Comisiones de Valores.
OTF	<i>Organized trading facility</i> . Sistema organizado de contratación.
P2P	<i>Peer to peer</i> . De igual a igual (persona a persona).
PAN	<i>Personal account number</i> . Número personal de 16 dígitos que se encuentra en las tarjetas.
PCI	<i>Payment Card Industry</i> . Industria de tarjetas de pago.
PDCA	<i>Plan, Do, Check, Act</i> . Planear, Hacer, Comprobar y Actuar.
Pilot	Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) N.º 600/2014 y (UE) N.º 909/2014 y la Directiva 2014/65/UE (Texto pertinente a efectos del EEE).
PISP	<i>Payments Initiation Service Provider</i> . Proveedor de servicios de iniciación.
PoA	<i>Proof of activity</i> . Prueba de actividad.
PoB	<i>Proof of burn</i> . Prueba de quemado.
PoS	<i>Proof of stake</i> . Prueba de participación.
PoSv	<i>Proof of stake velocity</i> . Prueba de velocidad.
PoW	<i>Proof of work</i> . Prueba de trabajo o esfuerzo.
PSD I o DSP I	Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE.
PSD II o DSP II	Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.
PSP	<i>Payment Service Provider</i> . Proveedores de servicios de pago.
PSU	<i>Payment Services User</i> . Usuario de servicios de pago.
QR	<i>Quick response</i> . Código de respuesta rápida. Según la organización de consumidores y usuarios, es una etiqueta óptica que contiene información y puede ser leída por una máquina.

<b>Abreviatura</b>	<b>Significado</b>
RBA	<i>Risk-based approach</i> . Enfoque basado en riesgos.
RDL	Real Decreto Ley.
<i>retail CBDC</i> o <i>rCBDC</i>	Moneda digital de banco central enfocada a público general (minorista).
ROFIEG	<i>Expert Group on Regulatory Obstacles to Financial Innovation</i> . Grupo de expertos en obstáculos regulatorios a la innovación financiera.
RPA	<i>Robotic Process Automatization</i> . Automatización robótica de procesos.
RTS	<i>Regulatory technical standards</i> . Estándares técnicos regulatorios.
SAFT	<i>Simple agreement of future tokens</i> . Acuerdo de futuras fichas.
SART	<i>Significant asset-referenced token</i> . Fichas significativas referenciadas a activos.
SCA	<i>Strong customer authentication</i> . Autenticación reforzada de cliente.
SEC	<i>Securities Exchange Commission (US)</i> . Comisión de bolsa y valores norteamericana.
SEMT	<i>Significant e-money token</i> . Fichas significativas de dinero electrónico.
SEPA	<i>Single Euro Payments Area</i> . Zona de pagos únicos europea.
SLA	<i>Service Level Agreement</i> . Acuerdo de nivel de servicios.
SNCE	Sistema Nacional de Compensación Electrónica.
SPEI	Sistema de Pagos Electrónicos Interbancarios de México.
SSI	<i>Self-Sovereign Identity</i> . Identidad autónoma soberana.
STO	<i>Security Token Offering</i> . Oferta de <i>tokens</i> de valores.
STP	<i>Straight Through Processing</i> . Procedimiento de operaciones automáticas.
SWIFT	<i>Society for Worldwide Interbank Financial Telecommunication</i> .
SWIFT RMA Key	<i>SWIFT Relationship Management Application Keys</i> .
TARGET 2	<i>Trans-European Automated Real-time Gross Settlement Express Transfer System</i> .
TIBER-EU	<i>European framework for threat intelligence-based ethical red-teaming</i> . Marco europeo para equipo rojo ético basado en inteligencia de amenazas
TIC	Tecnologías de la información y la comunicación.
TIPS	<i>TARGET Instant Payment Settlement</i> . Sistema de liquidación automática de TARGET.
TLPT	<i>Threat-led penetration testing on live production</i> . Pruebas de penetración dirigidas por amenazas en producción en vivo.
TPP	<i>Third Party Service Provider</i> . Terceras Partes Proveedoras de Servicios de Pago (incluye agregadores e iniciadores, esto es, AISP y PISP).

<b>Abreviatura</b>	<b>Significado</b>
TPV	Terminales de puntos de venta.
UAE	<i>United Arab Emirates</i> . Emiratos Árabes Unidos.
UCITS	Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM).
V.V.A.A.	Varios autores.
VLOP	<i>Very large on-line platform</i> . Plataforma en línea de gran tamaño.
VLOSE	<i>Very large on-line search engines</i> . Motores de búsqueda en línea de gran tamaño.
VUCA	<i>Volatility, uncertainty, complexity and ambiguity</i> . Volatilidad, incertidumbre, complejidad y ambigüedad.
wBTC	<i>Wrapped bitcoin</i> o bitcoin envuelto.
WEF	<i>World Economic Forum</i> . Foro Económico Mundial.
wholesale CBDC o wCBDC	Moneda digital de banco central enfocada en el sector mayorista (pagos interbancarios).

**UNIVERSO *FINTECH*: DE LA EVOLUCIÓN A LA DISRUPCIÓN DE LA  
TECNOLOGÍA EN FINANZAS. MARCOS DE SUPERVISIÓN Y  
REGULACIÓN**

**INTRODUCCIÓN**



## INTRODUCCIÓN

*“El mundo era tan reciente, que muchas cosas carecían de nombre, y para mencionarlas había que señalarlas con el dedo”*

(García, 2007, p. 1)

### I. CONTEXTO, RELEVANCIA Y OBJETIVOS

La innovación y las nuevas tecnologías son temas que cada vez aparecen más en los discursos de los bancos centrales y supervisores, no solo de la Unión Europea (UE), sino a nivel global (Bank of International Settlements [BIS], 2020c, p.88). Sin embargo, la innovación tecnológica en finanzas comenzó en el siglo XIX con la implementación del cable de comunicaciones transatlántico que unía a Estados Unidos con Europa, facilitando el comercio internacional y, por lo tanto, los movimientos financieros entre los continentes.

Las cuestiones por abordar, entonces, son saber a partir de cuándo la innovación en finanzas ha llevado a cabo una metamorfosis que la ha transformado en un elemento disruptivo, cuáles han sido sus desencadenantes, qué implica esto desde el punto de vista de los entornos de producción normativa y los marcos de supervisión, especialmente en la zona europea, y, finalmente, cuáles podrían ser las soluciones para afrontar estas nuevas realidades tan fluidas y dinámicas.

La literatura de investigación en torno a la temática de innovación tecnológica (*FinTech*) aún es emergente en los entornos financieros, centrándose en aspectos económicos o en la identificación de su potencial y riesgos. En lo que respecta a los estudios puramente legales, por lo general, estos suelen enfocarse en un nicho o vertical específica, como el *crowdfunding*, por ejemplo, Este tipo de investigaciones son aún más escasas en lengua española, especialmente en enfoques supervisores o cuando se extiende el estudio al ámbito de las llamadas finanzas descentralizadas o DeFi (modelos financieros basados en la tecnología de registros distribuidos (DLT) que prescinden de la figura de terceros de confianza).

Fuente de búsqueda	Tipo de documento	Idioma	<i>FinTech</i>		
			Total	Ciencias jurídicas	Temática principal supervisión
Dialnet	Tesis	Español	10	3	0
		Inglés	NA	NA	NA
	Revistas	Español	177	62	13
		Inglés	34	3	0
	Libros	Español	13	8	0
		Inglés	2	1	1
Fuente de búsqueda	Tipo de documento	Idioma	Total	Social Science	Temática principal supervisión
Scopus	Revistas	Español	10	8	1
		Inglés	1357	347	24
	Libros	Español	NA	NA	NA
		Inglés	43	7	1

Tabla 1. Resultados de búsqueda con la palabra “FinTech” en las bases de datos de Dialnet y Scopus a 14 de febrero de 2022

Nota. Elaboración propia.

La presente tesis incluye, en su primera parte, aportes novedosos en aspectos como el análisis y la delimitación del fenómeno *FinTech*, identificando los elementos que han provocado una disrupción de los modelos financieros tradicionales. Por lo tanto, resulta relevante cuestionarse cuándo la innovación pasó a ser un elemento de impacto en los mercados financieros y, por consiguiente, en los modelos de producción de políticas normativas y enfoques de supervisión. Es importante determinar a partir de qué momento la innovación financiera adquirió su propio término (*FinTech*) y qué se entiende exactamente por ello. Por este motivo, esta tesis abarca el periodo temporal de 1866 a junio de 2023, con un enfoque principal en las etapas en las que la innovación provocó una disrupción en los mercados (denominadas en este estudio como etapas *FinTech* 3.0, 3.5 y 4.0).

Además, este trabajo ofrece el valor añadido de un estudio y estructuración de los propios modelos *FinTech* en comparación con las operaciones de las instituciones financieras tradicionales, incluyendo la reciente irrupción de las Finanzas Descentralizadas (DeFi) en el panorama y los retos de supervisión que ello plantea. Este análisis en sí mismo supone una tarea constructiva, puesto que se está hablando de un concepto sobre el cual no existe consenso en cuanto a su definición, límites y características. La terminología utilizada es novedosa y alejada de los conceptos legales y financieros tradicionales, lo cual requiere una identificación clara antes de iniciar cualquier discusión sobre cómo afrontar estos desafíos. En suma, la novedad en sí de la



primera parte reside en llegar a definir y demarcar la innovación financiera de una forma estructurada.

En la segunda parte de esta tesis se abordan los enfoques normativos y de supervisión que se han aplicado a *FinTech* en la zona europea, con el fin de evaluar su adecuación ante una realidad que supone un cambio de paradigma.

De este modo, se defiende el argumento de que estas innovaciones están impactando en los modelos regulatorios y de supervisión actuales, los cuales requieren un replanteamiento adecuado a los nuevos tiempos. Desde el punto de vista normativo, se discute si *FinTech* supone la aparición de lagunas normativas y, por tanto, la necesidad de buscar soluciones como la aplicación analógica de normas, o si se está ante una manifestación tan radicalmente distinta que requiere su propia normativa e incluso un planteamiento distinto de supervisión en la zona euro.

Los principales desafíos a los que se enfrentan los reguladores son la rapidez, la constante evolución y el componente altamente tecnológico del fenómeno, que va más allá del perímetro regulatorio, planteando modelos en los que el código es la ley.

Es cierto que las soluciones inicialmente planteadas por el regulador han sido la extensión de la regulación existente con base en principios de analogía (*same activity, same risk, same rules*). Sin embargo, este trabajo busca demostrar que en muchas ocasiones no se trata de la misma actividad o mismos riesgos, lo que resulta en situaciones de alegalidad que requieren de nuevas soluciones normativas *ad hoc*. Esta tesis propone soluciones basadas en principios como la proporcionalidad, el enfoque basado en riesgos y “a prueba de futuro” para ser lo suficientemente ágiles y flexibles frente a ciclos de innovación constante cada vez más cortos.

En lo que respecta a la supervisión, los nuevos retos se centran en el hecho de que estos negocios no tienen fronteras y pueden ofrecerse a nivel mundial, sin que existan entidades legales o sujetos identificables en muchos casos (especialmente en las denominadas DeFi). Además, las finanzas basadas en tecnologías de registros distribuidos como *Blockchain*<sup>1</sup> no son censurables, lo que hace que las soluciones de supervisión actuales resulten inefectivas.

---

<sup>1</sup> *Blockchain*, o cadena de bloques, es un tipo específico de tecnología de registros distribuidos que organiza la información en bloques. Estos bloques están interconectados a través de claves criptográficas (*hash*) como un método de verificación para asegurar que la información no se ha manipulado. Puede definirse

No se trata únicamente de las innovaciones en sí, sino también de la cantidad de datos tratados y manejados. A modo de ejemplo, el Banco de Inglaterra, ya en 2019, recibía más de 65 billones de puntos de datos cada año en relación con las entidades supervisadas, suponiendo verdaderos retos para los equipos de inspección y supervisión. En palabras del gobernador del Banco Central, revisar esta información equivaldría a que cada supervisor tendría leer las obras completas de Shakespeare dos veces a la semana, durante todo el año (Carney, 2019, p. 9).

El motivo subyacente de la necesidad de nuevos planteamientos regulatorios y de supervisión se deben a que, hasta el momento, dichos modelos se han basado en estrategias de carácter evolutivo, con cambios que podrían catalogarse como análogos o lineares (la innovación se produce de forma paralela a los cambios regulatorios) (Barefoot, 2020, p. 5). Sin embargo, *FinTech* plantea un cambio de paradigma por el que se entra en una era digital, de cambio exponencial, lo que requiere nuevos enfoques y soluciones que puedan hacer frente a estas nuevas realidades. Esto se puede observar en la Figura 1, donde se compara la línea temporal con el aumento de la capacidad de incremento de las habilidades tecnológicas (Barefoot, 2020, p. 5).

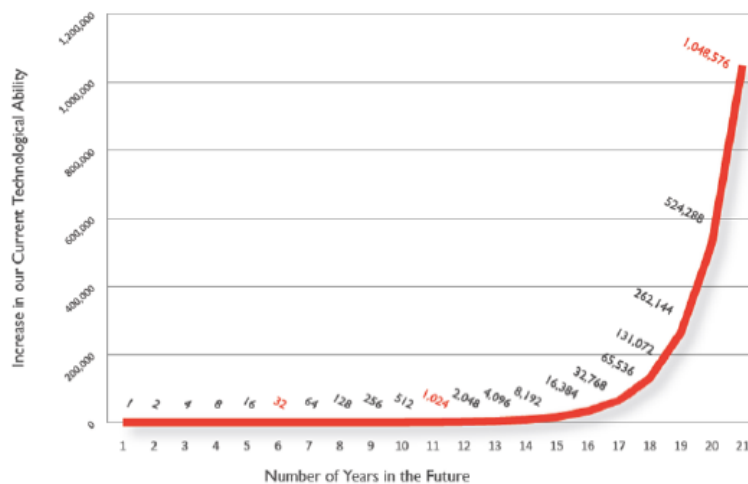


Figura 1. Evolución estimada de la capacidad tecnológica en 20 años

Nota. Adaptado de *Digitizing Financial Regulation: RegTech As A Solution for Regulatory Inefficiency and Ineffectiveness* (p. 5), por J.A. Barefoot, 2020,

[https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP\\_150\\_final.pdf](https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_150_final.pdf)

---

como “un libro de registro inmutable que contiene la historia completa de todas las transacciones que se han ejecutado en la red, a cada participante se le llama nodo, que en realidad viene a ser un ordenador más o menos potente” (Ortega, 2019, p. 24).

En lo concerniente a geografía, estudio se enfocó principalmente en la zona de la Unión Europea, pudiendo analizar otras jurisdicciones en determinados casos o con efectos de comparativa respecto a prácticas o estándares. Por tanto, los objetivos de esta tesis pueden resumirse en los siguientes puntos:

**Objetivo general:** el objetivo principal de este trabajo es analizar tanto el fenómeno *FinTech* como los enfoques regulatorios y de supervisión de este, con el fin de proponer soluciones de principios de marcos normativos y de supervisión.

Para ello, se proponen los siguientes objetivos específicos como soporte o desarrollo del objetivo general planteado:

- Objetivo específico 1: alcanzar una definición del concepto de *innovación tecnológico-financiera (FinTech)*.
- Objetivo específico 2: identificar las etapas de *FinTech*, sus características y los hitos que las marcan.
- Objetivo específico 3: identificar a partir de qué etapa *FinTech* se puede considerar que la innovación ya no es parte de la evolución en finanzas, sino que se vuelve una disrupción de estas.
- Objetivo específico 4: analizar los modelos de negocio de las fases de disrupción *FinTech* en comparativa con los modelos financieros tradicionales, así como sus enfoques normativos y las cuestiones que presentan.
- Objetivo específico 5: investigar las implicaciones de *FinTech* en los modelos de regulación y supervisión existentes, realizando un análisis crítico de las principales iniciativas regulatorias *FinTech* en los últimos años.
- Objetivo específico 6: evaluar si su encaje regulatorio y de supervisión actual es factible o si *FinTech* plantea un cambio del *statu quo* regulatorio y de supervisión.
- Objetivo específico 7: plantear soluciones de futura regulación y supervisión *FinTech*, así como los principios en los que deberán basarse.

## II. HIPÓTESIS DE INVESTIGACIÓN

La principal hipótesis de esta investigación se centra en el supuesto de que la disrupción *FinTech* está desbordando las estructuras de producción normativa y de

supervisión financiera, generando lagunas jurídicas. Por consiguiente, se hace necesaria una nueva formulación de modelos normativos y de supervisión.

Al igual que los objetivos, la hipótesis principal está soportada por varias hipótesis secundarias:

- Hipótesis secundaria 1: en la actualidad, *FinTech* está causando una disrupción en los mercados financieros.
- Hipótesis secundaria 2: los modelos *FinTech* provocan reinterpretaciones del concepto de tercero de confianza.
- Hipótesis secundaria 3: los marcos normativos actuales resultan insuficientes o parciales.
- Hipótesis secundaria 4: los marcos de supervisión actual resultan insuficientes o parciales.
- Hipótesis secundaria 5: las soluciones regulatorias y de supervisión deberán complementarse con normas *ex novo* y autocontrol del sector privado, en nuevas interpretaciones con claras connotaciones tecnológicas (el código como ley, la programación como arbitraje embebido).
- Hipótesis secundaria 6: la solución óptima sería aquella que ofreciera una regulación o controles mínimos desde el diseño de la propia tecnología.

### **III. METODOLOGÍA**

Este trabajo propone que *FinTech* representa un cambio de paradigma, es decir, una disrupción, y, por tanto, genera lagunas jurídicas que pueden ser tratadas vía métodos tradicionales (aplicación de la analogía) y mediante herramientas novedosas (*sandbox* regulatorios). Sin embargo, en ocasiones se hace necesaria la producción de marcos normativos específicos.

Con el fin de identificar cuándo estos nuevos marcos son necesarios, es imprescindible identificar qué es el fenómeno *FinTech* y cuáles son sus etapas (identificado como primera parte).

Esta tesis comienza llevando a cabo una delimitación y diagnóstico de la realidad *FinTech* con el fin de sentar las bases y obtener una imagen lo más precisa posible de la actualidad, previo a evaluar su problemática, dados los constantes cambios que vive esta

actividad. Así, un correcto entendimiento y definición de estos factores extrajurídicos contribuirá a sustentar los resultados del proyecto de investigación jurídica.

Si bien la aplicación de la extensión de normativas existentes mediante analogía puede haber sido una solución inicial, no deja de ser una salida temporal que deviene (cada vez más) insuficiente. Este enfoque provisional es válido solo cuando cabe hablar de la misma actividad o sustancia equivalente a la regulada, que presenta riesgos equivalentes a los supervisados.

Así, la aplicación de la analogía contaría con una finalidad de extensión regulatoria de normativas de los Estados Miembros, que descansaría sobre principios de equivalencia funcional y equivalencia regulatoria.

La equivalencia funcional consistiría en la identidad en la función, por la que la regulación en una determinada materia se aplica a una nueva área. Por otro lado, la equivalencia regulatoria considera que la norma aplica al supuesto innovador (actividad *FinTech*) en base a que ambas contemplan una finalidad regulatoria similar de protección o punición.

Sin embargo, como se expone a lo largo de este trabajo, cada vez hay más actividades sustancialmente diferentes debido al papel que la tecnología juega en ellas, lo cual altera su ADN y su estructura de riesgos. De esa manera, se generan situaciones de actividad de carácter financiero cuyo marco normativo es incierto, lo que podría catalogarse como alegal al no estar contempladas en el sistema legal actual (Coalition of automated legal applications, 2021, p. 5).

Por tanto, como se estudia en el “CAPÍTULO V. SUPERVISIÓN FINTECH: LA TEORÍA DEL DESFASE SUPERVISOR”, el principio de misma actividad, mismo riesgo, misma regulación no siempre es aplicable, demandando una nueva metodología de regulación y supervisión. En consecuencia, se propone una investigación jurídico-propositiva en la que se plantean principalmente modificaciones y la creación de nuevos fundamentos jurídicos de la norma (Tantaleán, 2016, pp. 8-9).

Para soportar la argumentación de la necesidad de un cambio de estrategias normativas y de supervisión, se lleva a cabo una acotación del fenómeno *FinTech* y se argumenta por qué los nuevos modelos son disruptivos mediante su estudio y comparación. Asimismo, se delinean los nuevos principios que deben fundamentar la producción normativa futura, la cual debe adoptar un enfoque de balance entre la agilidad y la seguridad jurídica.

#### IV. ESTRUCTURA

En cuanto a la estructura, se presenta una introducción, seguida de dos bloques principales y una conclusión. La primera parte se enfoca en el estudio del fenómeno *FinTech*, desde su demarcación y definición hasta su evolución y disrupción. Después de identificar y delimitar el fenómeno, la segunda parte aborda los principales desafíos desde la perspectiva de la supervisión y regulación, proponiendo un rediseño basado en principios para lograr mayor dinamismo y capacidad de respuesta.

La **introducción** tiene como objetivo acercar al lector a la cuestión del fenómeno *FinTech* como tema de relevancia en la escena financiera actual. También establece las reglas del juego de esta investigación al presentar los objetivos e hipótesis iniciales. Además, se formula el contexto metodológico de la investigación, que incluye la identificación y delimitación (primera parte) y el estudio teleológico (problemática de las lagunas en regulación y supervisión, posibilidad de aplicación por analogía, conclusión de la necesidad de nuevos modelos normativos y de supervisión, así como la propuesta de estos) en la segunda parte.

De esta manera, en esta introducción se busca dibujar el alcance del trabajo de investigación, indicar la metodología utilizada y destacar que los fenómenos disruptivos implican un cambio en el método de legislarlos y supervisarlos, requiriendo, en ciertos casos, de diseños totalmente nuevos o *ad hoc* (las denominadas leyes marco).

La **primera parte**, que se centra en el fenómeno *FinTech*, se divide en cuatro capítulos.

El primer capítulo de la primera parte realiza un análisis de la literatura sobre la definición del concepto de *FinTech*, para el cual no existe actualmente un acuerdo o estandarización. Luego se procede a identificar los elementos principales que deben incluirse en el concepto para formular una definición adecuada para los fines de esta investigación. A continuación, se examinan los esfuerzos en el análisis de *FinTech* desde diversas perspectivas de las partes involucradas.

Una vez formulada la definición y exploradas las distintas perspectivas, se examina cómo *FinTech* puede ofrecer respuestas a cuestiones presentes en los modelos financieros tradicionales. Además, se expone una diferenciación de etapas de *FinTech*, denominadas *FinTech* 1.0 (1866-1960), *FinTech* 2.0 (1960-2008), *FinTech* 3.0-3.5 (2008-2020) y *FinTech* 4.0 (2020 en adelante).

La mayoría de la literatura Rincón (2021, pp. 82-83); Antoneus et al. (2021, pp- 371-378); Brummer (2020); Arner (2016, pp. 1-33); Zunzunegui et al. (2019, p. 22) identifica estas tres etapas en los avances tecnológico-financieros, aunque puede haber ligeras diferencias en la duración de cada periodo. Por lo general, se considera que la primera etapa (*FinTech* 1.0) abarca los años 1866 a 1967 Brummer C. extiende hasta los 2000) (Brummer, 2020, pp. 10-15). La segunda etapa, denominada *FinTech* 2.0, abarca desde 1967 a 2008. Finalmente, toda la literatura analizada coincide en que la evolución *FinTech* continúa en la tercera etapa 3.0 a 3.5, considerada desde 2008 hasta la actualidad.

Como novedad a los estadios identificados hasta la fecha, este trabajo considera que a partir del año 2020 se pueden identificar indicios de una nueva etapa (denominada *FinTech* 4.0 o cuarta etapa), caracterizada por la eclosión de las DeFi, nuevas formas de organización (como las DAO) y los criptoactivos, que son objeto de análisis en su correspondiente capítulo (CAPÍTULO IV). Estos elementos soportan una nueva realidad de mayor envergadura e impacto jurídico, como es el Metaverso.

El segundo capítulo gira en torno a los albores de la introducción de innovaciones y nuevas tecnologías en el sector financiero. Estos periodos iniciales engloban ciclos de evolución carentes de elementos suficientemente disruptivos (etapas de *FinTech* 1.0 y 2.0). Igualmente, se analizan los modelos regulatorios y de supervisión preponderantes en estas épocas, considerando la falta de coordinación a nivel europeo durante gran parte del periodo.

Dado que el componente de interés es la disrupción, estas etapas no se consideran altamente relevantes, por lo que se abordan de manera conjunta. Son fases cerradas con agentes similares (instituciones financieras reguladas) y soluciones normativas y de supervisión tradicionales que ofrecen respuestas adecuadas a las innovaciones, debido a la velocidad y la baja frecuencia de eventos.

El tercer capítulo de la primera parte se centra en las primeras etapas de disrupción, diferenciando entre la etapa *FinTech* 3.0, cuyo epicentro fue la UE mediante la implementación de modelos de banca abierta en el ámbito de los pagos; y la etapa *FinTech* 3.5, cuyo desarrollo se ha llevado a cabo principalmente en otras regiones como Asia o América Latina a través de la implantación de constructos de finanzas abiertas. Estos sistemas de finanzas abiertas son más extensivos, puesto que abordan cuestiones más allá

de los pagos. Por lo tanto, van un paso más allá del actual modelo europeo, motivo por el cual *FinTech 3.5* hace numerosas referencias a regiones fuera de la UE.

Tanto *FinTech 3.0* como *FinTech 3.5* se identifican como etapas de una desintermediación centralizada. En otras palabras, se produce la entrada de nuevos agentes distintos a las entidades financieras tradicionales, que fragmentan la cadena de valor a través de la especialización. Sin embargo, estos nuevos agentes aún se basan en modelos societarios y operativos tradicionales.

Los componentes disruptivos de este ciclo se centran en la entrada de nuevos actores, especialmente las grandes empresas tecnológicas (analizadas con mayor detalle), y la concentración de distintas soluciones innovadoras en un corto periodo de tiempo, que pueden aplicarse a las finanzas (tanto para los clientes como en las infraestructuras). Estas innovaciones son de diversa naturaleza impactando en numerosos aspectos del mundo financiero (ver figura ejemplificativa a continuación)

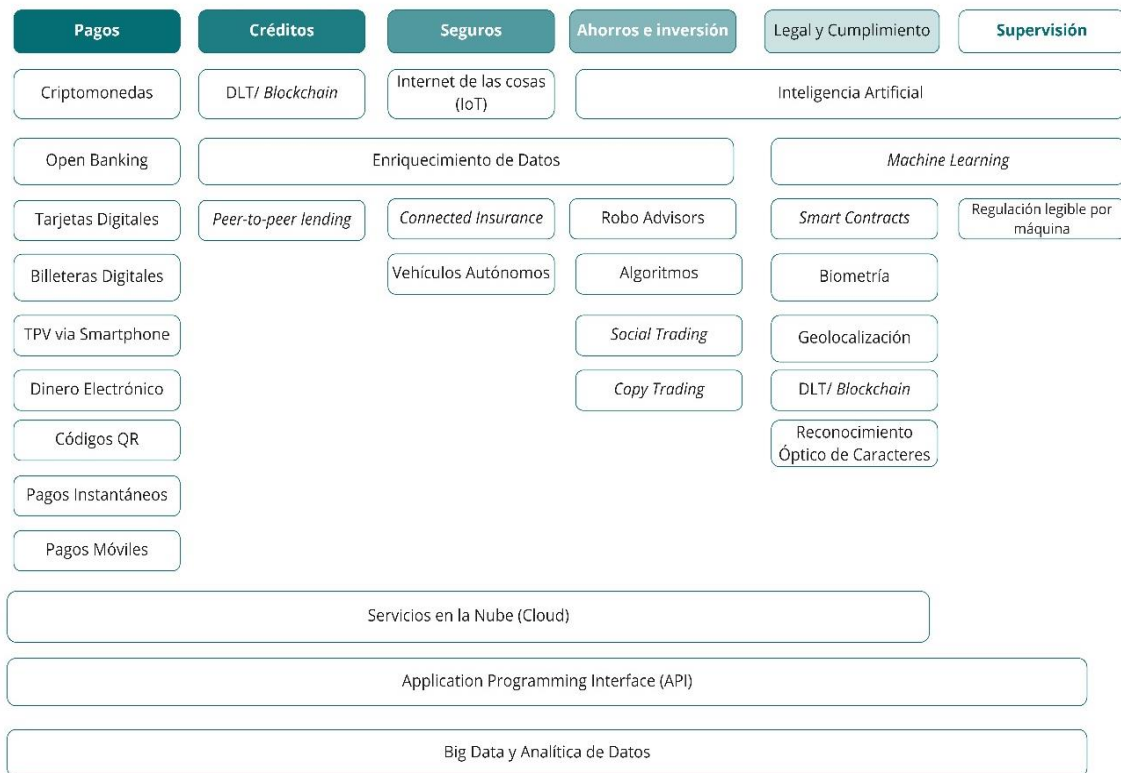


Figura 2. Ejemplos de disrupciones tecnológicas en el sector financiero

Nota: elaboración propia.



Esto implica que entidades que realizan actividades similares no estén reguladas en casos en los que deberían estarlo (especialmente cuando se trata de regulaciones enfocadas a entidades –*entity based*– en las que hay listas cerradas de sujetos obligados). En este caso se analizan en profundidad tanto los sujetos como las actividades, identificando sus componentes novedosos y si están regulados o no.

Esta disrupción no es tan radical como en la etapa *FinTech* 4.0, que se aborda en el cuarto capítulo y que, como se verá, ofrece el potencial de prescindir de las figuras tradicionales de concentración (ya sea un banco central o una institución financiera regulada).

El cuarto capítulo de la primera parte cubre el periodo *FinTech* 4.0, que engloba las denominadas DeFi, que confían en el código o la tecnología para llevar a cabo actividades financieras. Como resultado de este enfoque, surgen los criptoactivos, cuya taxonomía se estudia en este capítulo, puesto que representan la “sangre” de estos nuevos mercados financieros. Tanto DeFi como los criptoactivos tienen sus raíces en la tecnología de registros distribuidos (DLT), siendo *Blockchain* la forma más conocida de esta tecnología.

Es precisamente esta tecnología descentralizada la que proporciona un componente disruptivo significativo (la capacidad de prescindir de modelos centralizados dependientes de terceros de confianza). Este rasgo es el que genera la principal disrupción en el mundo financiero 4.0. No obstante, la banca tradicional también está experimentando con estos nuevos activos y modelos de negocio, buscando determinar cuál será su papel en estas finanzas del futuro.

Finalmente, se realiza una aproximación a cómo DeFi encaja dentro de los nuevos mundos y universos virtuales. Es decir, los metaversos como ecosistemas de soporte de las DeFi y la necesidad de que se regulen.

Una vez se ha definido *FinTech* y delimitados sus modelos de manera cronológica, la **segunda parte** de la tesis aborda la incertidumbre que este fenómeno implica en modelos de supervisión y regulación. Asimismo, se proponen posibles bases o pilares para nuevos modelos más flexibles que permitan adaptarse con mayor rapidez a la situación actual. Por lo tanto, la segunda parte se centra en deliberaciones sobre cómo regular y supervisar fenómenos disruptivos que representan un cambio de paradigma en la industria financiera.

El quinto capítulo de la segunda parte estudia los modelos de regulación y supervisión *FinTech* actuales, proponiendo lo que se ha denominado en este trabajo como la teoría del desfase supervisor. Como consecuencia de ello, se establecen potenciales soluciones de estrategias normativas y de supervisión (principios para una nueva ley marco), sugiriendo modelos colaborativos público-privados en los que exista cierto nivel de delegación de las entidades sujetas a supervisión con el fin de alcanzar otras contrapartes que podrían estar sujetas a una suerte de supervisión indirecta o privatizada. Asimismo, se debate sobre posibles soluciones de supervisión incrustada o por diseño, que podrían basarse en el principio de que el código es la ley.

El sexto capítulo se centra en reflexiones sobre los modelos de regulación *FinTech*, incluyendo si estos modelos deben regularse, el potencial de una regulación marco, el planteamiento de nuevos regímenes de licencias para los agentes que realizan estas actividades, los posibles nuevos sujetos obligados y la cuestión que plantean estas actividades, es decir, la aparición de lagunas normativas que pueden ser temporalmente solventadas mediante el mecanismo de la analogía, pero que, debido a su materialidad, a menudo requieren normativa *ex novo*.

Como muestra de ello, el capítulo séptimo realiza un análisis crítico de las principales iniciativas de política regulatoria que se han desarrollado en la actualidad, distinguiendo entre soluciones de normativas *ad hoc*, esto es, el Reglamento sobre los Mercados de Criptoactivos (MiCA o MiCAR), el Reglamento del Régimen Piloto de DLT (Pilot) y el Reglamento de Resiliencia Operativa del Sector Financiero (DORA). Igualmente, se lleva a cabo una aproximación hacia la regulación *ad hoc* transversal, no financiera, como el *Digital Markets Act* (DMA) y el *Digital Services Act* (DSA).

Por otra parte, se llevan a cabo pequeños análisis de iniciativas de revisión de piezas regulatorias existentes relacionadas con la identidad digital soberana (eIDAS) en aquellos aspectos de impacto en el mundo financiero y la ideación de un posible desarrollo o evolución de la segunda directiva de servicios de pago (PSD II). Estas regulaciones se evalúan desde el punto de vista de los principios identificados como clave en esta tesis, para concluir que dicha regulación, incluso en borradores o recientemente publicada, no se adecua a las necesidades actuales y, por tanto, nace o nacerá obsoleta en ciertos aspectos debido a la rigidez de los modelos normativos existentes en la actualidad. Seguidamente, se reflexiona sobre las nuevas soluciones de experimentación supervisora que han emergido a lo largo de los últimos años, como los *hub* de innovación o los

denominados *sandbox* regulatorios<sup>2</sup>, discutiendo si se trata de una solución estratégica o una simple herramienta de aprendizaje.

Finalmente, se presenta una **conclusión** identificando los principales hitos y hallazgos de esta investigación, así como futuras vías de exploración. En todo caso, este estudio aspira a ofrecer una exploración comprensiva del fenómeno *FinTech* en la actualidad, aportando claridad sobre la extensión que estos modelos están teniendo y sus implicaciones regulatorias y de supervisión. Asimismo, se aspira a ofrecer posibles escenarios alternativos frente a las cuestiones que estas innovaciones están planteando, dado que suponen un reto al estar en continua metamorfosis.

Pese a que el principal foco de este trabajo se ha delimitado a la UE, con el objetivo de estudiar las finanzas abiertas de manera comprensiva, y debido a que dichos modelos aún no se dan en la zona europea, *FinTech 3.5* versará eminentemente sobre ejemplos de otras regiones, como América Latina o Asia.

Debido a la novedad del tema, aún existe escasa doctrina o jurisprudencia sobre la materia. Por este motivo, el análisis en este aspecto se ha centrado en casos globales, incluyendo ejemplos estadounidenses, en los que los supervisores y tribunales han sido más activos y que, por tanto, podrían sentar precedentes como referencia para tener en cuenta en la UE.

---

<sup>2</sup> Instrumento puente que permite a las entidades privadas examinar en producción sus modelos novedosos a la par que las autoridades alcanzan un mayor entendimiento de estos, siendo capaces de este modo de asesorar sobre la posible necesidad de nuevas interpretaciones de la regulación existente o el desarrollo de normativas *ad hoc*.



**PRIMERA PARTE: EL FENÓMENO *FINTECH***



## CAPÍTULO I. CONSIDERACIONES PREVIAS

Este capítulo de apertura de la primera parte (fenómeno *FinTech*) pretende mostrar la cuestión que se presentó desde el inicio, es decir, la falta de consenso sobre qué es *FinTech*. En ese sentido, en primer lugar, se realiza un análisis de las distintas definiciones (doctrina, organismos e instituciones), para llegar a una definición propia. En segundo lugar, se lleva a cabo una aproximación de lo que implica el término desde diferentes perspectivas, abriendo el debate sobre si se está frente a un cambio de paradigma o una simple evolución de actividades que ya existían en el pasado. En tercer lugar, se identifican cuáles son los elementos diferenciadores de esta nueva actividad respecto a las finanzas tradicionales. Finalmente, se presentan las etapas *FinTech*, las cuales se abordan en los capítulos siguientes dentro de esta primera parte constructiva.

### I. DEFINICIÓN

Con el propósito de abordar el objeto de estudio y plantear una definición adecuada, el primer paso consistió en delimitar y sustanciar el concepto de *FinTech*. Por este motivo, se llevó a cabo una revisión de la literatura, seleccionando un total de 25 definiciones de diversas fuentes. El objetivo fue identificar si existe un acuerdo común respecto al concepto y sus características (ANEXO II).

En este proceso, se buscó identificar y catalogar dichas acepciones en función de si se centran en una actividad innovadora o si parten de una perspectiva basada en la entidad legal. Además, se evaluó si las definiciones contienen términos relacionados con la disrupción, como “materialidad”, “impacto” o “relevancia”, dado que este estudio aborda la discusión sobre si *FinTech* es un fenómeno disruptivo.

Por otra parte, se analizó si el enfoque del que parte es amplio o si se centra en determinados aspectos del *FinTech*. Por ejemplo, algunas definiciones pueden abordar únicamente el fenómeno desde la perspectiva del público general, sin tener en cuenta las innovaciones en infraestructuras que pueden proporcionar ventajas indirectas a los consumidores e inversores finales. Tras evaluar estas definiciones, se concluyó que actualmente no existe un acuerdo sobre la definición del concepto de *FinTech*, siendo los únicos elementos comunes los relacionados con la semántica del propio término, esto es: finanzas (*financial*) y tecnología (*technology*).

Realizando un análisis de las posibles definiciones del concepto *FinTech*, se identificaron dos tipos de acepciones que, para efectos de este trabajo, se denominaron como “orientados a entidad” (*entity oriented*) u “orientados a innovación” (*innovation oriented*). La primera acepción, *entity oriented* (24 % de definiciones analizadas) hace referencia a un tipo de entidades en concreto (“las *FinTech*”, entidades *FinTech* o *FinTech firms*) que realizan actividades con un corte claramente tecnológico en relación con actividades financieras y auxiliares.

Una parte de estas entidades ya vendrían contenidas en actividades que venía realizando un subsector de la banca tradicional, la denominada “banca en la sombra” (*shadow banking*) (Rodríguez, 2019). Sin embargo, al hablar de entes jurídicos con personalidad propia, se podría considerar que este significado excluye las innovaciones que puedan haberse aplicado dentro de la banca tradicional (*incumbents*) y, por lo tanto, se evaluaron como parciales para los fines de este trabajo.

Volviendo a la definición de las entidades *FinTech*, se considera que puede incluir tanto aquellas empresas cuyo modelo de negocio se centra en la oferta de servicios financieros a través de la implementación de nuevas tecnologías y que surgen sin ningún legado regulatorio o tecnológico previo (entidades *FinTech*), como aquellas empresas cuyo modelo de negocio original es la tecnología misma y que se diversifican hacia el ámbito financiero (entidades *TechFin*). Dentro de esta última categoría se encuentran las denominadas *BigTech*, que son gigantes tecnológicos que han mostrado su interés por el mundo financiero. Estas figuras se analizan en el apartado de las *BigTech*.

La estrategia de origen y evolución de estos agentes se puede apreciar en la Figura 3 a continuación.



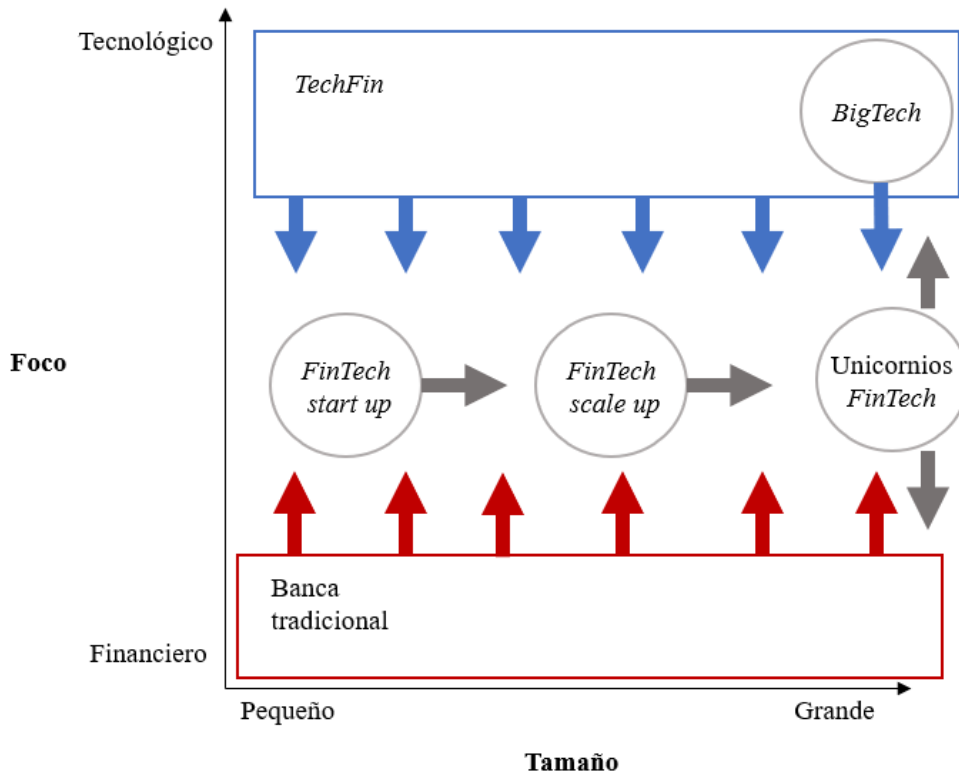


Figura 3. Agentes en la industria financiera actual. Estrategias de origen y evolución en función de su tamaño y foco

Nota: elaboración propia.

Como se observa en la Figura 2, las entidades que parten de la industria tecnológica han aprovechado su capacidad de innovación y desarrollo en los últimos años para expandir su rango de capacidad hacia vertientes subyacentes como la financiera. Por esta razón, se les denomina *TechFin*. Dentro de las *TechFin*, la mayor parte de la discusión en el plano regulatorio y de supervisión se ha fundado en las denominadas *BigTech*, que son entidades de gran tamaño procedentes del ámbito tecnológico y que, en su gran mayoría, se basan en un modelo de negocio de plataformas *online*.

Por otro lado, también han surgido nuevos agentes con un perfil híbrido, que combinan tecnología y finanzas. Estas entidades buscan crecer, pasando de ser *start-ups* o empresas emergentes de *FinTech* a escalar y finalmente obtener la denominación de “unicornios *FinTech*”, esto es, *FinTech* valoradas en más de 1 000 000 000 USD. Una vez alcanzan estos tamaños, pasan a competir con las *BigTech* y las grandes instituciones financieras. Es importante señalar que la banca tradicional también se ha visto impactada por la entrada de nuevos participantes y la disrupción de la innovación. Así, ha adoptado

distintas estrategias, que se analizarán más adelante, con el fin de avanzar hacia la transformación digital.

La Figura 3 muestra que el concepto de *FinTech* es algo que va más allá de una entidad y, por lo tanto, la definición debe abordarse desde el segundo enfoque que se analiza a continuación.

Volviendo a los dos tipos de definiciones mencionados anteriormente, el segundo enfoque del concepto *FinTech*, orientado a la innovación (*innovation oriented*), es más amplio, puesto que abarca avances aplicados en el sector financiero que generan un impacto en el mercado, independientemente de la contraparte que las lleve a cabo o que se encuentre afectada. Este segundo planteamiento parece ser el más aceptado según la mayoría de los documentos analizados (72 % de la muestra tomada). Únicamente en casos excepcionales (4 %), se mencionan ambos (entidades y actividades), distinguiendo entre *FinTech* y entidades *FinTech*, y definiendo estas acepciones claramente.

Por otro lado, aspectos e indicadores de otros términos clave, como si se trata de un enfoque amplio o específico, o si se hace referencia a acepciones indicativas de disrupción, materialidad, impacto o relevancia, se vuelven residuales o menores en estas definiciones como se verá a continuación.

Para esta investigación, se consideró fundamental determinar en qué momento se puede distinguir entre una simple evolución y una disrupción *FinTech*. En este sentido, la definición debe incluir conceptos como la materialidad (presente o futura) del impacto en la industria. Sin embargo, el 72 % de las definiciones analizadas no mencionaban palabras como disrupción, materialidad, impacto o relevancia, lo que implica que cualquier cambio tecnológico aplicado a las finanzas podría considerarse *FinTech*, independientemente de su impacto en la industria. La falta de inclusión de elementos que cataloguen la envergadura del impacto puede derivar en un concepto no representativo o demasiado amplio de *FinTech*, por lo que, para el planteamiento de una definición propia, se considera crucial incluir esta característica.

Por último, se evaluó si las descripciones del término comprendían no solo la provisión de servicios financieros enfocados al público, sino también innovaciones de infraestructuras o servicios administrativos. En ese orden de ideas, el 40 % de las definiciones son amplias o genéricas, sin llegar a un nivel de detalle específico. Solo se identificó un caso en el que expresamente se asoció el término *FinTech* no solo a la

provisión de servicios de cara a clientes (*front office*), sino también con actividades internas, administrativas y contables (*back office*).

En conclusión, para fines de este trabajo, el fenómeno *FinTech* se definió como el desarrollo de innovaciones tecnológicas en entornos digitales con impacto material real o potencial en la industria financiera y, por ende, en sus infraestructuras y participantes (consumidores, entidades, instituciones financieras y autoridades).

Este concepto permite incluir nuevas modalidades enfocadas a cumplimientos regulatorios (*RegTech*), legales (*LegalTech*) o de supervisión (*SupTech*). Además, es lo suficientemente amplio para abarcar nuevos conceptos que están eclosionando actualmente y que ya están generando impacto en la industria financiera, como los criptoactivos o las DeFi, que no requieren de una entidad jurídica o emplean nuevas formas de organización en las que el código es el corazón y las personas pasan a adoptar roles secundarios (las denominadas organizaciones autónomas descentralizadas [DAO])<sup>3</sup>.

En cuanto al elemento de materialidad real o potencial incluido en la definición propuesta, es importante considerar qué tipo de cambios implicarían un cambio material o potencialmente material para el sector financiero. Este término debe mantenerse deliberadamente abierto, dado que debe ser flexible para hacer frente a la constante evolución de la tecnología. El concepto de materialidad debe adaptarse y no puede ser universal en su totalidad, puesto que debe contener cierto grado de ambigüedad o incertidumbre que será abordado por los criterios supervisores en cada momento.

Si bien existen pautas base de materialidad que pueden servir de referencia<sup>4</sup>, es necesario mantener un listado abierto para poder contemplar situaciones no previstas que puedan generarse por las innovaciones tecnológicas en finanzas. No existe un único concepto totalitario de materialidad, y este debe tratarse con base en unos elementos básicos (por ejemplo, número de jurisdicciones afectadas o cuotas de mercado), sujetos a la interpretación de supervisores financieros con el fin de adquirir la agilidad suficiente como para poder abordar los riesgos cambiantes que se presentarán a futuro.

---

<sup>3</sup> Las DAO surgen como forma de organización alternativa dentro de las DeFi, que emplean un método de pago disruptivo (criptoactivos) y generan actividades y experiencias en nuevos mundos digitales (el metaverso). Todos estos conceptos se desarrollan a lo largo de esta tesis.

<sup>4</sup> Por ejemplo, que el servicio sea subyacente a la operativa general de las instituciones financieras, que el servicio sea requerido por la gran mayoría de la población para garantizar la protección al consumidor, que el servicio pueda tener un impacto significativo en el control de riesgos sistémicos, o que pueda suponer un riesgo generalizado en términos de crimen financiero y requiera medidas para prevenir abusos, o que pueda representar un riesgo de abuso de mercado.

La definición propuesta también permite dar cuerpo a distintos estadios por los que pasa el concepto de *FinTech* en sí, marcado por cambios tecnológicos con incidencia en distintos aspectos en función del panorama temporal que se esté tratando. Por tal razón, en función de la materialidad del cambio y de la erosión en el *statu quo*, se podrá hablar de evolución *FinTech* o verdadera disrupción *FinTech*.

De esa manera, esta definición podría abarcar el fenómeno e incluir perspectivas en las que existe falta de acuerdo, debido a que los participantes tienen puntos de partida diferentes en términos de tamaño, función, uso e implicaciones, como se discutirá a continuación.

## **II. LA INNOVACIÓN TECNOLÓGICA: EVOLUCIÓN O CAMBIO DE PARADIGMA**

Actualmente, es difícil delimitar el concepto de *FinTech* por varios motivos. En primer lugar, las innovaciones en las que se basa están en constante cambio y desarrollo, lo que hace complicado establecer los límites de lo que se considera innovaciones financieras. Además, los agentes o *stakeholders* que están involucrados en el universo *FinTech* también están en constante evolución y parten de distintos puntos de vista respecto al fenómeno.

Por esta razón, el término *FinTech* puede tener diferentes interpretaciones dependiendo del punto de vista o perspectiva desde la cual se analice (Clark, 2021), lo que plantea la discusión sobre si se trata de una evolución en las finanzas o una verdadera disrupción y cambio de paradigma. Esta distinción es importante, dado que una evolución implica modificaciones en los marcos regulatorios existentes o interpretaciones amplias de estos, mientras que una disrupción requiere la creación de nuevas regulaciones debido a lagunas o vacíos normativos. Por lo tanto, se realizó una primera aproximación desde las diferentes perspectivas de los actores involucrados y sus argumentos para considerar a *FinTech* como una evolución o una disrupción.

### **1. Instituciones financieras establecidas (*incumbents*): argumento evolutivo**

Si se contempla el concepto *FinTech* desde la perspectiva de las instituciones financieras ya establecidas (denominadas *incumbents*), podría considerarse que la aplicación de innovaciones tecnológicas en el mundo de las finanzas para generar cambios en el sector no es algo novedoso que haya florecido en la última década. El uso

de la tecnología como desencadenante de cambios materiales en finanzas podría remontarse a los años 60 con la aparición de los cajeros automáticos (*Automated Teller Machine*, ATM) (Shepherd-Barron, 2017, pp. 1-3). Esta innovación permitió, en su momento, eliminar la dependencia de los horarios de apertura al público de las entidades financieras, lo que permitía acceder al servicio de retirada de dinero en cualquier momento del día. A esta invención le han seguido otras que ahora se podrían considerar como innovaciones tecnológicas de primera generación, como el télex, el fax y, posteriormente, las negociaciones de alta frecuencia (*high frequency trading*).

A medida que los desarrollos tecnológicos iban avanzando y la capacidad computacional de los ordenadores mejoraba, se acumulaba cada vez más información que las entidades del sistema financiero tradicional no explotaban o procesaban. Este ha sido uno de los focos *FinTech* de las entidades financieras a lo largo de los últimos años, buscando ofrecer soluciones al público de gestión y optimización de sus finanzas. Además, los medios de consumo de servicios financieros han mudado de la presencialidad hacia la operativa a través de banca en línea (en formato web o de aplicación en un teléfono inteligente).

Este desplazamiento hacia la explotación de datos y la digitalización de usuarios requiere una reevaluación de las estrategias empresariales, ya sea mediante la reestructuración de la infraestructura tecnológica y la contratación de perfiles informáticos, o a través de la colaboración con empresas *FinTech*. En definitiva, desde el punto de vista de las instituciones financieras establecidas, el fenómeno *FinTech* no representa una revolución, sino una evolución, una tendencia que ya estaba presente en la banca desde hace tiempo, pero que ha experimentado un crecimiento exponencial en la última década. Esta postura se basa en el reconocimiento de que el sector financiero siempre ha sido uno de los principales consumidores de tecnología.

## **2. Emprendedores en el sector (*start-ups*): argumento de disrupción**

Desde el punto de vista de las entidades emprendedoras que han emergido en el sector a lo largo de los últimos años, el pistoletazo de salida en la UE se marcó a raíz de la Segunda Directiva de Servicios de Pago (PSD II)<sup>5</sup> y sus normas de desarrollo. Esta

---

<sup>5</sup> Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) 1093/2010 y se deroga la Directiva 2007/64/CE (Texto pertinente a efectos del EEE)

directiva marcó un antes y un después en términos de apertura de datos de pago de los clientes, incorporando el concepto de *banca abierta* (*open banking*) que se analiza en detalle en capítulos posteriores.

Antes de su entrada en vigor, los datos financieros de los bancos no se compartían debido a requerimientos de confidencialidad y secreto bancario. Esto provocaba que la gestión de las finanzas desde el punto de vista del individuo estuviera desagregada, dificultando la capacidad de tener una imagen completa de la situación patrimonial y de tomar decisiones de optimización respecto a esta. Por tanto, para las *FinTech start-ups* europeas, el fenómeno tiene sus orígenes en la apertura de los datos de pago, a través de la cual los usuarios recuperan parcialmente el control sobre sus datos. Esto genera una oportunidad de negocio mediante el uso de interfaces de programación de aplicaciones, conocidas como API. Esta apertura de los datos a los clientes es un factor de soporte de *FinTech* como disrupción, puesto que ha generado cambios profundos en los hábitos de los consumidores financieros.

Al igual que en el caso de las instituciones financieras establecidas, el uso de teléfonos móviles y el aumento de los servicios en línea ha permitido que estas entidades desarrollen nuevas ideas de customización y reducción de costes mediante el uso de nuevas tecnologías. Esta reducción de costes beneficia no solo a los consumidores finales, sino que también beneficia a los bancos en esquemas de colaboración entre las *start-ups* y las instituciones financieras.

En virtud de ello, *FinTech* supone nuevas experiencias de cara a consumidores finales y el público en general, eminentemente digitales y ya no limitadas a una computadora o un ordenador portátil, sino moviéndose hacia teléfonos móviles o incluso los denominados *wearables* (por ejemplo, finanzas desde un reloj inteligente). En resumen, para las *FinTech start-ups* se trata de una revolución en la forma de concebir las finanzas, que se ha desarrollado principalmente a lo largo de la última década.

### **3. Entidades tecnológicas en finanzas (*TechFin*): la disrupción de las masas**

Las entidades tecnológicas ya establecidas han venido proporcionando distintos tipos de servicios a las entidades financieras. Con el tiempo, la dependencia de estas instituciones hacia las empresas tecnológicas ha ido aumentando, convirtiéndose en proveedores críticos de las instituciones bancarias. Específicamente, para el subgrupo de empresas tecnológicas de gran tamaño (denominadas *BigTech*), la apertura de datos

financieros ha supuesto una oportunidad de salto a una industria que contaba con barreras de entrada elevadas. Esta apertura les ha permitido monetizar su capacidad de explotación y análisis de datos, así como aprovechar las economías de escala basadas en su infraestructura tecnológica global. Estas *BigTech* se desarrollarán más adelante en detalle.

La aparición de las *TechFin* en la industria financiera agrega una capa adicional de complejidad al desarrollo de políticas públicas de supervisión, debido a que son modelos que operan en numerosas jurisdicciones al mismo tiempo, lo que dificulta establecer los límites tanto geográficos como de actividad en los que los supervisores tradicionalmente han trabajado.

Al igual que sucede con las *FinTech start-ups*, los cambios acontecidos a lo largo de estos 10 años se interpretan como un cambio de paradigma, debido a que se les ha permitido acceder a una industria tradicionalmente cerrada. Esto ha generado nuevos negocios y ha ampliado la base de clientes con acceso a servicios financieros *online* que antes no eran rentables. Para estos clientes, su relación no es con un banco, sino con una empresa tecnológica, como una plataforma o una aplicación. Además, estos cambios no se limitan a una región específica, sino que tienen un efecto global. Por ejemplo, cabe imaginar el impacto masivo que tendría si la aplicación de WhatsApp ofreciera su propia billetera digital.

En el caso de las *TechFin*, el cambio de paradigma debe a la apertura de datos financieros de clientes, así como de actividades tradicionalmente reservadas a instituciones financieras. Así, se permite la explotación y el servicio en el ámbito financiero por entidades históricamente no reguladas, desdibujando los límites de industrias.

Además, se plantean ventajas competitivas, especialmente para estos nuevos agentes, debido a que sobresalen en su capacidad de tratamiento y explotación de datos, previsión de necesidades y expectativas de usuarios, junto con sus efectos de red y amplia base de clientes. Estas palancas son herencia de los servicios ya prestados a nivel mundial en sectores tecnológicos, entretenimiento, compras en línea, comunicaciones o transporte.

De hecho, se generan situaciones de vacíos regulatorios o de regulaciones no proporcionales a los riesgos que las *TechFin* plantean, dado que se accede y explotan datos, generando actividades similares o equivalentes a las financieras, pero careciendo de normativa aplicable a estos actores.

#### 4. Perspectiva del público: consumidores e inversores no institucionales

Para los consumidores, la aparición del fenómeno *FinTech* ha supuesto un cambio en la forma de gestionar su patrimonio de manera inmediata, fácil, segura y reduciendo sus costes. En concreto, las generaciones nativas digitales (generación X, Y, Z) se caracterizan por una mayor confianza en la tecnología en contraste con su desconfianza en la banca, que fue el origen de la crisis económica de 2008 (Pradel y Hochedez, 2022; pp.1-4; Cherrayil, 2021). Por este motivo, *FinTech* representa para estos usuarios una forma de gestionar sus finanzas sin depender de los bancos, una contraparte de la que no se fían.

Desde el punto de vista del público como inversores, *FinTech* ha permitido el desarrollo de nuevas formas de inversión a través de modelos novedosos, como el *crowdfunding* o los criptoactivos. Estas opciones han ganado una mayor participación en el mercado en los últimos años debido al potencial retorno de la inversión en comparación con los mercados tradicionales. Además, estas operaciones no necesariamente requieren de cantidades mínimas para participar y sus procesos de conocimiento del cliente y evaluación de idoneidad son más ágiles en el caso del *crowdfunding*, e incluso pueden ser inexistentes en el caso de los criptoactivos. Por lo tanto, desde la perspectiva del público no institucional, *FinTech* representa un fenómeno que ha incrementado su adopción a raíz de la crisis financiera, ofreciendo soluciones tecnológico-financieras alternativas a los esquemas tradicionales de finanzas que resultan más atractivas para las audiencias digitales.

La capacidad de prescindir de un tercero de confianza o de los criterios de un banco central, y la libertad de cualquier individuo a emitir su propia moneda digital, debe considerarse un fenómeno disruptivo. Específicamente en el caso de los criptoactivos (analizados en la etapa *FinTech* 4.0), este fenómeno no tiene precedentes y su impacto en consumidores y usuarios es potencialmente global, planteando importantes riesgos que aún no están contemplados normativamente. En ese sentido, los criptoactivos se convierten en una suerte de competidor del dinero de curso legal, provocando una descentralización y desintermediación de pagos de los bancos centrales a entidades privadas e incluso individuos. Como consecuencia de ello, los bancos centrales han reaccionado mediante la creación de las denominadas monedas digitales de bancos centrales o *Central Bank Digital Currencies* (CBDC).



## **5. *FinTech* desde la perspectiva de los reguladores y supervisores: afrontar el fenómeno**

Los reguladores y supervisores han visto cómo sus marcos normativos y de supervisión se han vuelto obsoletos en poco tiempo debido a que *FinTech* tiene varias implicaciones de alto impacto para estas contrapartes. Este cambio se debe a una combinación de factores, siendo los principales: (i) la entrada de nuevos agentes que realizan actividades que podrían estar sujetas a regulación, (ii) el rápido desarrollo de numerosas innovaciones que afectan al sector, (iii) la naturaleza global de estos modelos de negocio, que desafían la capacidad de supervisión y detección de actividades ilícitas, y (iv) la aparición de modelos híbridos y fraccionados en las cadenas de valor financieras, lo que dificulta la comprensión y el asesoramiento integral de los riesgos asociados a estos negocios.

Por lo tanto, es necesario buscar nuevas fórmulas para un mejor entendimiento de los riesgos y oportunidades que *FinTech* presenta no solo para el mercado, sino también para las propias instituciones. *FinTech* supone un desafío tanto positivo como negativo para los reguladores y supervisores, y aún se necesita determinar su alcance, los límites y las actividades que deben estar sujetas a mandatos regulatorios y de supervisión. Este aspecto en particular se explorará con mayor detalle en el presente estudio de investigación.

### **III. PROBLEMÁTICA DE LAS FINANZAS TRADICIONALES Y *FINTECH* COMO SU RESPUESTA**

El concepto de *FinTech* como alternativa al sector financiero tradicional ha ganado fuerza especialmente después de las crisis financieras globales. *FinTech* plantea la posibilidad de ofrecer soluciones alternativas en las que se confía en nuevos agentes que parecen atraer a públicos más digitales y, en algunos casos, incluso permiten prescindir de roles centralizados que han sido ampliamente criticados por el papel jugado en las crisis financieras.

En este contexto, se comienza a evaluar qué ha fallado y cuáles son los principales puntos débiles del ecosistema hasta el momento. De acuerdo con Campbell R. Harvey (Campbell et al., 2021), se identificaron cinco conceptos que *FinTech* busca mejorar en comparación con los esquemas tradicionales. Estos conceptos son: (i) control centralizado, (ii) limitación de acceso, (iii) ineficiencia, (iv) falta de interoperabilidad y (v) opacidad. A continuación, se plantea cómo *FinTech* es una respuesta a estas carencias.

## 1. Control centralizado

El control centralizado puede observarse tanto desde la esfera pública como desde la privada. Históricamente, las políticas monetarias, fiscales, la inflación y la emisión de dinero han estado bajo el control de las autoridades y los bancos centrales. De manera similar, la oferta privada de servicios financieros estaba limitada a los participantes del sistema bancario, el cual en el caso europeo siempre se ha caracterizado por una alta concentración en un reducido número de agentes. Por lo tanto, se podría hablar de un monopolio en la emisión de moneda de curso legal y un oligopolio en la distribución y oferta de servicios financieros, donde el acceso presenta barreras significativas desde el punto de vista de la competencia, lo cual ha llevado a constantes reestructuraciones y fusiones en los grupos financieros.

En lo que respecta a este último punto (concentración desde el lado privado), las entidades *FinTech* que han surgido principalmente desde 2008 en adelante han contribuido a erosionar la concentración de servicios ofrecidos por la banca comercial, incrementando la competencia no solo en número de agentes, sino también mediante el aumento de la oferta de servicios y la reducción de costes para la clientela.

En cuanto a la concentración o monopolios del lado público, no es hasta lo que se denomina la etapa *FinTech* 4.0 (DeFi) que se han materializado las ideas que se presentan como alternativas al *statu quo* actual. En esta fase, cobra mayor fuerza el uso de criptoactivos<sup>6</sup> de emisión privada y servicios relacionados con ellos, cuya operación e infraestructura no están controladas por los gobiernos locales ni las autoridades.

## 2. Limitación de acceso

La concentración de servicios financieros en un limitado número de entidades financieras, junto con los cada vez más altos costes regulatorios impuestos a las mismas, ha llevado a tomar decisiones estratégicas centradas en el mantenimiento de aquellos mercados, clientes y divisiones que sean rentables y sostenibles. Por lo general, este tipo de decisiones juega en contra de los colectivos más desfavorecidos o de los países en desarrollo, donde el costo de hacer negocios es mayor al potencial beneficio que puedan

---

<sup>6</sup> “Representaciones digitales de valor habilitados por la criptografía y la tecnología de registros distribuidos” (Su, 2020, p. 2). “Una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar” (art. 3.1.5) de MiCA).

brindar. Como resultado, se produce una limitación en el acceso y uso de prestaciones de calidad para ciertos colectivos y regiones.

Actualmente, los servicios financieros no se están disponibles en su totalidad para todo el mundo. Esto se debe a varias razones, como la delimitación operativa por jurisdicción, los requerimientos normativos que exigen asegurarse de que el producto es adecuado al perfil del cliente, los costes asociados a la actividad o el hecho de que se busque clientela que sea rentable para la entidad financiera. Por tanto, se crean limitaciones específicas por jurisdicciones y regiones en términos de criterios normativos, prudenciales (capital, solvencia y liquidez) y de negocio, lo que aumenta el coste y conduce a una reducción de la oferta física presencial (oficinas, personal, horarios) y la base de clientes.

La limitación de acceso ha sido históricamente uno de los elementos fundamentales del desarrollo de innovaciones en las finanzas. De hecho, la aparición del ATM marcó el comienzo de la etapa (que se identificará como *FinTech 2.0*). Las iteraciones posteriores en *FinTech* se han centrado en reducir estas barreras de acceso mediante la automatización de procesos y la reducción de costes asociados a la necesidad de contar con oficinas físicas y personal para ofrecer el producto. Adicional a ello, la explotación de datos ha permitido un mejor conocimiento de los colectivos no atendidos o mal atendidos, lo que ha llevado a reevaluar su elegibilidad para acceder a la actividad, como, por ejemplo, financiación y capacidad de pago.

La universalización y verdadera globalización de las finanzas en su máxima expresión se está alcanzando con las DeFi, donde cualquier persona con acceso a internet puede acceder desde cualquier parte del mundo a la actividad que necesite, con una amplia oferta y sin verse limitada por su perfil, historial crediticio u otras condiciones.

### **3. Ineficiencia**

Viene siendo generalmente reconocido que las estructuras financieras clásicas adolecen de ineficiencias debido a la fragmentación de infraestructuras. Dicha fragmentación se hace patente, por ejemplo, en los casos de transferencias internacionales, donde se requiere la participación de numerosos agentes para procesar las transacciones de principio a fin (Bank of International Settlements, 2021a; Financial Stability Board [FSB], 2020d, pp.1-34). Estas ineficiencias se reflejan en términos de tiempos de procesamiento, volúmenes de operaciones manejadas y costos.

En ese orden de ideas, *FinTech* se presenta como una solución alternativa, reduciendo la carga operativa manual o proponiendo nuevas formas de operar que permiten el acceso a nuevos colectivos. Por ejemplo, en el campo de la inversión, que estaba limitado a individuos con cierta capacidad financiera y asesorados por agentes con los correspondientes costos asociados. *FinTech* introduce la automatización del asesoramiento a través de los llamados asesores automatizados o *robo-advisors*, lo que reduce el tiempo necesario para tomar decisiones, el seguimiento de la operación y el costo del producto en sí, al eliminar costos generales de mano de obra.

Más recientemente, se ha producido una transformación radical de la arquitectura a través de la cual se realizan las operaciones financieras, mediante el uso de la tecnología de cadenas de bloques (DLT) como alternativa a los sistemas utilizados hasta ahora. Esta tecnología permite que, si el público detecta ineficiencias en el propio producto ofrecido, se pueda reutilizar la idea y la tecnología para desarrollar una alternativa mejor de forma libre. Es decir, los servicios son reutilizables por cualquier persona, puesto que se trata de estructuras abiertas que promueven la libre competencia y la mejora continua de la eficiencia financiera.

#### **4. Falta de interoperabilidad**

Parte de las ineficiencias descritas anteriormente devienen de un problema más estructural de los esquemas financieros clásicos: su falta de interoperabilidad. Ello deriva en la necesidad de empleo de distintos canales para procesar una operación, sufriendo las consecuencias de estos fraccionamientos. Un claro ejemplo de esta cuestión se refleja en los sistemas de transferencias internacionales, que comprende la infraestructura de pagos del país de origen, los canales de pago internacionales y la infraestructura de pagos del país de destino. Estos flujos e ineficiencias se estudiarán en detalle en el capítulo de banca abierta (CAPÍTULO III).

La falta de interoperabilidad se extiende también a los propios servicios financieros. Por lo general, existía una endogamia en el sector, lo que significa que los productos solo eran compatibles si pertenecían a la misma entidad financiera. Esto se debía, en parte, a que se trataba de operaciones cerradas en las que los datos no se compartían.

No fue hasta la aparición de la red de comunicación interbancaria SWIFT que se desarrolló una solución operativa para la gran mayoría de países e instituciones participantes en transferencias internacionales. Sin embargo, SWIFT también implicaba

la concentración de poder en una única entidad que establecía *de facto* las reglas del juego, lo que generaba un punto único de concentración y posibles fallos. Además, SWIFT no se utiliza a nivel local, dado que cada país tiene una o varias soluciones que funcionan como vías o canales para procesar operaciones financieras, a menudo incompatibles entre sí o sin mecanismos adecuados de interoperabilidad.

Con la llegada de la banca abierta para los servicios de pago a través de la Segunda Directiva de Servicios de Pago (PSD II), se desarrollaron mejoras en las infraestructuras existentes y una clara apertura de los datos bancarios de pagos en la zona europea, permitiendo una mejor experiencia de usuario. Además, el desarrollo de interfaces de programación de aplicaciones brindó la posibilidad de compartir información financiera y, asimismo, comparar los productos de distintas entidades. Estas opciones, que simplemente requerían conectarse y comenzar a funcionar, alcanzaron su máxima expresión con el desarrollo de todo un ecosistema financiero paralelo basado en la tecnología de registros distribuidos.

## **5. Opacidad**

La falta de transparencia de la banca tradicional ha sido objeto de críticas constantes por parte de las autoridades, lo que ha llevado a tomar medidas para garantizar que se divulguen al público los márgenes y comisiones que se les cobran, así como los incentivos que reciben las entidades por recomendar ciertos productos de terceros (un ejemplo de esto es el artículo 24 de MiFID II<sup>7</sup>).

Hitos tales como la introducción de la banca abierta (para pagos) y las finanzas abiertas (para servicios financieros en general) han arrojado luz sobre estos aspectos mediante la aparición de comparadores de productos, que son aplicaciones que permiten a los usuarios comparar la oferta de servicios de diferentes entidades, sus precios y comisiones. De nuevo, es en la etapa más reciente de las DeFi donde se alcanza la máxima transparencia en términos de costos, puesto que la tecnología utilizada es completamente transparente, lo que permite cualquier persona auditar toda la transacción y sus costos si tiene los conocimientos técnicos necesarios.

---

<sup>7</sup> Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (versión refundida) Texto pertinente a efectos del EEE.

Como puede verse, *FinTech* aborda posibles soluciones que cubrirían aquellas debilidades que han sido punto de crítica de los modelos de negocios financieros hasta la fecha: (i) control centralizado, (ii) limitación de acceso, (iii) ineficiencia, (iv) falta de interoperabilidad y (v) opacidad.

## CAPÍTULO II. ANTECEDENTES: *FINTECH 1.0* Y *FINTECH 2.0*

### I. INTRODUCCIÓN

Como se argumentó anteriormente, las etapas *FinTech 1.0* y *FinTech 2.0* son estadios temporales de evolución interna de la banca, propulsada por la introducción de cierto tipo de innovaciones que llevan las finanzas a otro nivel, pero no llegan a causar una disrupción. A continuación, se identifica la fase *FinTech 1.0*, caracterizada por la importancia del *hardware* y cuyo hito principal fue la interconexión entre países a ambos lados del Atlántico. Seguidamente, se estudia el estadio *FinTech 2.0*, en el que se identifica una concentración de oportunidades en servicios de pago y sus infraestructuras.

Ambos periodos temporales (de 1866 a 2008) se caracterizan por lo que se denomina “modelos tradicionales de banca y supervisión” (también conocido como *TradFi* o *CeFi*<sup>8</sup>), en los que la actividad está reservada y sujeta a normativa, cuya aplicación es evaluada con posterioridad por las autoridades mediante el esquema de inspección física. El liderazgo de estas etapas es asumido por los países desarrollados, dado que son el foco de la aplicación de innovación en el mundo financiero (para más detalle, ver ANEXO III).

### II. *FINTECH 1.0*: EL *HARDWARE* Y LA INTERCONEXIÓN DE PAÍSES

La etapa *FinTech 1.0* se caracteriza eminentemente por el desarrollo de soluciones *hardware*<sup>9</sup> y de infraestructuras, inicialmente aplicables de forma generalizada, y que generaron un impulso para el mundo financiero. A medida que avanza el tiempo, comienzan a surgir innovaciones específicas de infraestructuras financieras.

La puesta en marcha del primer cable telegráfico transoceánico en 1866 es considerada por la doctrina (Cárdenas, 2021, pp. 82-83; Sorongan et al., 2021, pp. 371-375; Brummer, 2020; Arner, 2016; Zunzunegui et al., 2019, p. 22), como el avance que marcó un progreso en las finanzas al conectar Estados Unidos con el Reino Unido (Müller y Tworek, 2015, pp. 259 - 283). Este hito, unido al ferrocarril y el barco de vapor, agiliza los trámites del comercio y las operaciones financieras asociadas a estos. Es por esto por lo que, a lo largo

---

<sup>8</sup> *TradFi* significa *traditional finance* o finanzas tradicionales y *CeFi* significa *centralized finance* o finanzas centralizadas.

<sup>9</sup> Según la RAE, *hardware* se define como “voz inglesa que se usa, en informática, para designar el conjunto de los componentes que integran la parte material de una computadora u ordenador”.

de las etapas *FinTech*, las innovaciones e hitos pasan de ser generales o exógenos en *FinTech 1.* a ser específicos y endógenos a la industria en *FinTech 2.0* y siguientes. Incluso, la innovación que marca el hito avanza de las instituciones establecidas (bancos) hacia los nuevos entrantes en *FinTech 3.0* a *4.0* (*FinTech* y las organizaciones autónomas descentralizadas que se abordan más adelante).

Fue precisamente la explotación del telégrafo lo que permitió la creación de Fedwire en 1918 (Arner, 2016, pp. 1-33), lo que habilitó la operativa interbancaria de los bancos pertenecientes a la Reserva Federal de Estados Unidos sin necesidad de transporte de fondos físicos o en efectivo. El mecanismo empleado por Fedwire se basaba en el uso de claves morse para las transferencias de fondos entre sus 12 bancos miembros (Theiyer Report, 2022, p.1). Este reconocimiento del impacto que la tecnología está teniendo en el sector financiero y las nuevas cuestiones para el público se hace patente en el propio discurso de aceptación de la reelección como presidente de Franklin D. Roosevelt en 1936:

*La era de la maquinaria, de los ferrocarriles; de vapor y electricidad; el telégrafo y la radio; producción en masa, distribución en masa: todo esto se combinó para hacer surgir una nueva civilización y, con ella, un nuevo problema para quienes buscaban permanecer libres.*

*Los nuevos reinos se construyeron sobre la base de la concentración del control sobre las cosas materiales. A través de nuevos usos de corporaciones, bancos y valores, nueva maquinaria de la industria y la agricultura, del trabajo y el capital —todos nunca soñados por los padres— toda la estructura de la vida moderna quedó impresa en este servicio real. (Roosevelt, 1936, pp. 1-6)*

La Segunda Guerra Mundial supuso la aceleración de mecanismos relacionados especialmente con la criptografía, la comunicación y los sistemas. Estas innovaciones comenzaron a ser adoptadas por la banca a través de los primeros usos de ordenadores.

En 1942, John Maynard Keynes planteó posibles soluciones de estructuras de pago internacionales. Propuso principalmente la creación de una Unión Internacional de Liquidación (*International Clearing Union*), cuyos miembros serían los bancos centrales de las naciones que se adhirieran al proyecto. Incluso, este fallido plan planteaba el nacimiento de una nueva moneda (*bancor*) que se emplearía para liquidaciones mayoristas entre los miembros (Ugolini, 2017, p. 85). Esta formulación, como se verá en



capítulos posteriores, se ha retomado en la actualidad bajo soluciones de criptodivisas emitidas por bancos comerciales para pagos mayoristas entre grupos de bancos (actualmente conocidas como CBDC sintéticas mayoristas).

Las innovaciones *FinTech* más relevantes para los consumidores finales de la época eran de carácter *hardware*, a través de las tarjetas de crédito. La primera tarjeta de crédito Diners Club se emitió en 1950. Esta innovación supuso un cambio en la forma de acceder al crédito al consumo por parte del público, y se amplió aún más con la aparición del Interbank Card Association (hoy conocida como MasterCard) en 1966 (Arner et al., 2015, p.8). Hacia finales de este periodo, las redes de Télex habían avanzado en Estados Unidos, Canadá, Reino Unido, Alemania y Francia, permitiendo el progreso del mundo financiero (Theiye Report, 2022, p.1).

En resumen, esta época se caracteriza por una introducción de la innovación tecnológica en el sector financiero, con origen exógeno a la propia industria. Esta fase es denominada “*mechanized banking introduced*” por Mishra (2009, p.4). Es precisamente esta introducción de la innovación lo que provocó la denominada “destrucción creativa” de Schumpeter, en la cual las nuevas tecnologías emergen destruyendo la productividad de modelos generados por tecnologías anteriores, ya sea desde la perspectiva física o desde la perspectiva de beneficios (Mazzucato y Wray, 2015, pp. 5-12).

### **III. FINTECH 2.0: LOS SERVICIOS DE PAGOS Y SUS INFRAESTRUCTURAS**

Hay elementos comunes entre *FinTech* 1.0 y 2.0, como pueden ser el alto nivel de centralización en entidades financieras tradicionales, lo que desemboca en altas barreras de acceso a la actividad financiera y la concentración de esta en países desarrollados. Sin embargo, existen elementos distintivos que hacen que los autores mencionados coincidan en la identificación de un nuevo ciclo en las finanzas (Cárdenas, 2021, pp. 82-83; Sorongan et al., 2021, pp. 371-375; Brummer, 2020; Arner, 2016; Zunzunegui et al., 2019, p. 22).

La era *FinTech* 2.0 viene marcada principalmente por mejoras en el sector de servicios de pagos e infraestructuras. Se observan innovaciones frontales con impacto directo en el público, y continúan los desarrollos de soluciones para la mejora de la interoperabilidad en las infraestructuras financieras, lo que beneficia directamente a las instituciones miembros e indirectamente a sus clientes.

*FinTech* 2.0 comenzó con una innovación financiera que transformó el sector de pagos: el ATM. Esta invención de John Sheperd-Barron se implementó por primera vez en 1967 en una sucursal de Barclays Bank en Enfield, al norte de Londres (Barclays, 2017; BBC News Mundo, 2021). Este invento *hardware* permitió solventar dos problemas de la banca: la experiencia de usuario y la seguridad. Hasta el momento, el público estaba sujeto a las limitaciones de la presencialidad en dos sentidos: (i) para realizar cualquier operación bancaria era necesario acercarse a la oficina y (ii) solo se podían realizar los trámites correspondientes dentro de determinados horarios (llegar tarde, como le sucedió a Sheperd-Barron, implicaba tener que acercarse otro día y haber perdido el tiempo).

En ese orden de ideas, el ATM supuso una sustancial mejora en la experiencia de usuario al liberarlo de la atadura de horarios para retirar efectivo. Este principio de desobstrucción siguió siendo el hilo conductor que condujo al desarrollo de servicios como la banca telefónica y la banca *online*, diseñados con el objetivo de reducir fricciones para los usuarios al contratar productos bancarios.

El segundo problema resuelto fue la seguridad. Debido a que las transacciones se realizaban de forma remota (sin interacción con un empleado del banco), existía un riesgo inminente de fraude: cómo asegurar que la persona que realizaba el retiro de fondos era realmente el propietario de la cuenta. Fue así como surgió el uso del PIN, que todavía se emplea en la actualidad.

La llegada de los teléfonos y ordenadores de uso privado, así como la conexión a internet en la década de los ochenta y noventa, habilitó nuevos canales de acceso al público. Esto dio lugar al surgimiento de la banca telefónica y banca *online*, permitiendo una mayor libertad a los usuarios, quienes cada vez más prescindían de la necesidad de presencialidad en las oficinas bancarias.

En lo que respecta a infraestructuras financieras, a lo largo de este periodo se implementaron los sistemas de compensación y liquidación centralizados, como *Bankers Automated Clearing Service* (BACS) en Reino Unido en 1968 y *Clearing House Interbanks Payment System* (CHIPS) en Estados Unidos en 1970, y se desarrollaron soluciones privadas de interoperabilidad a nivel internacional, como SWIFT en 1973 (Arner, 2016, pp. 1-33). El BACS es una red formada por los mayores bancos de Reino Unido junto con otras entidades reguladas (*building societies*) que han desarrollado una serie de estructuras y soluciones en torno a las infraestructuras de pago en el país. Entre

ellas se encuentra *Clearing House Automated Payment System* (CHAPS), que es un sistema de pagos alternativo al propio BACS. De forma similar a BACS, el CHIPS americano también permitía agilizar y simplificar el procedimiento de compensación entre los bancos neoyorquinos. Posteriormente, en 1971, apareció el *National Association of Securities Dealers Automated Quotations* (NASDAQ), permitiendo que, mediante el uso de la tecnología, las compañías pudieran financiarse a través de los mercados públicos (Theiher Report, 2022, p.1).

Siguiendo con las evoluciones en infraestructuras de pagos, la llegada de SWIFT en 1973 y su efecto de red (239 bancos de 15 países) supuso un paso adelante hacia un sistema de pagos global (SWIFT, 2022b). Además, en 1977 se sustituyeron las comunicaciones vía Télex por un modelo basado en mensajes (comúnmente llamados mensajes SWIFT) que permitía compartir un mayor nivel de datos, así como distinguir distintos tipos de mensajes (se diferenciaban mensajes de transferencias, transacciones interbancarias y otros, como cartas de crédito). Asimismo, en la década de los ochenta, comenzaron a identificarse ciertas herramientas de análisis y explotación de datos financieros y de mercados en la banca de inversión, de la mano de Bloomberg (Britannica, 2022).

En la UE, comenzó a vislumbrarse la necesidad de un Mecanismo Único de Supervisión (MUS), ya señalado en la Comunicación de la Comisión COM (1999) 232, del 11 de mayo de 1999 (Commission of European Communities, 1999). En esta comunicación se expone la necesidad de establecer un sistema de supervisión financiera europeo y promover la cooperación regional en lugar de la bilateralidad.

Para la región europea, esta fase se cerró con dos importantes hitos que dieron paso a la era *FinTech* 3.0. Uno de ellos fue la implementación en 1999 de sistemas de compensación bruta en tiempo real transeuropeos (*Trans-European Automated Real-time Gross Settlement Express Transfer System* o TARGET). TARGET se define como el diseño por parte del Eurosistema de una cámara de compensación y liquidación a la que solo acceden los bancos centrales de los Estados Miembros. A diferencia del programa estadounidense (*Federal Reserve System*), en el caso europeo los activos y pasivos netos de los bancos centrales nacionales no se liquidan (Ugolini, 2017, p. 84).

Tanto TARGET 1 como TARGET 2, implementado en 2007, representan un rediseño en una estructura centralizada que se sitúa por encima de las infraestructuras de pago locales, permitiendo una mayor interoperabilidad de los sistemas de pago en la región.

Acompañando a este cambio estructural, se publicó la Directiva 2007/64/EC, conocida como la Primera Directiva de Servicios de Pago (PSD I), que fijó por primera vez las reglas de los servicios de pago en la zona europea.

En conclusión, la era *FinTech* 2.0 comenzó centrándose en la innovación en infraestructuras operativas financieras, principalmente dirigidas a la industria financiera, y a medida que avanza, se extiende hacia las capas de consumidores. Desde el punto de vista de la supervisión, se evidencia cada vez más la necesidad de encaminar la supervisión hacia soluciones coordinadas a nivel regional.

#### **IV. ENFOQUES DE SUPERVISIÓN**

Pese a que tanto *FinTech* 1.0 como *FinTech* 2.0 brindaron cambios trascendentales tanto en las infraestructuras de mercados (mediante su interconexión) como en la libertad de los usuarios, no existe una ruptura o un fraccionamiento radical de las cadenas de valor en la oferta del servicio (se sigue manteniendo las finanzas en manos de las instituciones financieras tradicionales, por tanto, se habla de etapas de finanzas centralizadas TradFi o CeFi). Los negocios financieros se concentran en las grandes plazas de Estados Unidos, Reino Unido y Europa como regiones desarrolladas, siendo los principales beneficiarios el público ya bancarizado y las grandes empresas.

La actividad sigue estando en manos de la banca y, por tanto, los modelos de supervisión no varían en exceso. Además, nociones tales como el *enfoque basado en riesgos* o la *materialidad* no se observaron en Europa hasta la implantación de la normativa de Basilea II (2008), por lo que estos criterios no se aplicaron en los marcos regulatorios de la época. Los métodos de supervisión se enfocaban en la tradicional inspección o reacción regulatoria en caso de incidente, como fue el escenario americano con posterioridad al lunes negro de 1929.

De este modo, se identifica un antes y un después de los mecanismos de supervisión tras la crisis de 1929 y la finalización de la Segunda Guerra Mundial. Si bien, previo a estos hitos, la posición de los Estados se caracterizaba por un enfoque de liberalismo económico en el que las entidades participantes contaban con un alto margen de libertad, tras estos dos eventos, se hizo necesario un mayor nivel de intervencionismo por parte de las administraciones públicas mediante la delimitación del derecho público económico como instrumento de gestión de la estabilidad de los mercados financieros (Ortiz, 2017, pp. 21-36). En ese sentido, la época hasta 1929 estuvo influenciada por los pensamientos

de Adam Smith en su obra *La riqueza de las naciones* (Smith, 1776), permitiendo crecer los modelos financieros sin el control adecuado, en aras del crecimiento económico y la libre competencia, impulsando los ideales de los beneficios de la internacionalización y, posteriormente, la globalización.

Con posterioridad a la Segunda Guerra Mundial, Europa requirió de un esfuerzo de reconstrucción en mayor o menor medida, lo que condicionó los niveles de intervencionismo de los países de la actual UE y, a la postre, en sus sistemas bancarios. Estos aspectos incentivaron el desarrollo de normativas que delimitaron el perímetro de lo que se consideró actividad financiera, protegiendo este sector debido a su aspecto estratégico. En consecuencia, se generaron altas barreras de entrada por parte de nuevos participantes.

En conclusión, debido a que se trataba de épocas en las que las finanzas estaban limitadas a entidades financieras reguladas, no hubo una variación sustancial en los agentes objeto de supervisión. Las innovaciones se producen con tiempo suficiente como para reaccionar a tiempo y desarrollar o modificar la regulación requerida.



## CAPÍTULO III. HACIA EL CAMBIO DE PARADIGMA: *FINTECH* 3.0-3.5

### I. INTRODUCCIÓN

Este capítulo abarca dos etapas que han avanzado en paralelo en dos regiones. *FinTech* 3.0 comenzó en Europa con la apertura de los datos de pagos a terceras partes, y *FinTech* 3.0 se dio en regiones emergentes que hablaban directamente de apertura de datos a terceros en lo a que servicios financieros se refiere. Ambas etapas contaron con nuevos agentes *FinTech*, que se analizan como parte de la introducción. Posteriormente, se aborda la banca abierta en Europa y sus implicaciones disruptivas en pagos (*FinTech* 3.0), explicando los cambios que supone en entidades intervinientes y en las infraestructuras de estas actividades denominadas *PayTech*.

Con base en ello, se examinan las *PayTech* con impacto en el público, y se realiza una taxonomía de sujetos en función de distintos criterios, como son sus licencias o su actividad. A continuación, se lleva a cabo un estudio de cómo es la experiencia de los usuarios dentro de estas aplicaciones y una pequeña recapitulación sobre estos frontales de pagos. Una vez contempladas las innovaciones de cara a los clientes, se lleva a cabo una aproximación al impacto de la innovación en las infraestructuras de pagos, indicando las principales problemáticas existentes en la actualidad y los enfoques de acción público-privados, así como posibles soluciones. Por último, se realiza una evaluación de las implicaciones de estas iniciativas desde aspectos regulatorios y de gobernanza, y se concluye esta sección con una breve recapitulación en cuanto a las infraestructuras de pago.

Después de abordar la etapa *FinTech* 3.0 tanto en sujetos como en actividades (frontales y de infraestructuras), se procede a describir *FinTech* 3.5, esto es, las finanzas abiertas. Esta sección comienza con una reflexión sobre el cambio de la banca abierta a las finanzas abiertas, así como sus ventajas e inconvenientes. A continuación, se adopta un enfoque especial a un tipo particular de sujetos, como las grandes tecnológicas, debido al impacto que pueden tener en el universo *FinTech* y en las finanzas en general, así como a los desafíos regulatorios que plantean.

Al igual que en *FinTech* 3.0, una vez abordados los sujetos, se examina la transformación en las actividades, identificando dos tipos de transformación: una por verticales (es decir, servicios de pasivo, activo, productos de inversión y otros servicios)

y una transformación horizontal, que se da en los negocios “*as a service*” y que implican fragmentaciones en las cadenas de valor en finanzas.

Finalmente, se reflexiona sobre si esta fase supone verdaderamente una desintermediación o una simple reintermediación hacia nuevos terceros de confianza, motivo por el que esta tesis las denomina “etapas de descentralización centralizada” (CeDeFI). Similar a *FinTech 3.0*, se lleva a cabo un ejercicio de reflexión a modo de cierre de la sección.

### **1. Diferenciación entre *FinTech 3.0* y *FinTech 3.5***

El periodo *FinTech 3.0* está marcado a nivel mundial principalmente por dos efectos: la crisis mundial y la publicación del *paper* del que surgió la idea de Bitcoin en 2008. En lo que respecta a la zona europea, el año 2008 se caracteriza por el nacimiento de la *Single Euro Payments Area* (SEPA).

En general, esta etapa es eminentemente disruptiva a nivel global en varios aspectos: (i) la apertura, en mayor o menor medida, de los datos financieros de los usuarios, devolviéndoles el control y aumentando su capacidad de decisión; (ii) la aparición de numerosas innovaciones, como se observará al analizar los modelos de negocio *FinTech* en estas fases; y (iii) la apertura a nuevos proveedores de servicios, cuyo análisis en función de su origen y tamaño se realizará a continuación.

No obstante, es en esta fase donde se identifica un desacople de dos tipos: (i) entre los desarrollos normativos de la zona euro y los de los países emergentes, y (ii) entre los nuevos modelos de negocio *FinTech* y la normativa en sí.

Respecto al primer punto, la UE ha liderado principalmente el sector de pagos a lo largo de este período mediante la Primera y la Segunda Directiva de Pagos. Específicamente, la Segunda Directiva introduce la banca abierta (*open banking*), que devuelve la autonomía y la capacidad de decisión a los usuarios en asuntos relacionados con los pagos, y abre este sector a la entrada de terceros que históricamente no tenían acceso a estos datos debido a barreras regulatorias como la confidencialidad y el secreto bancario.

Sin embargo, los países emergentes han comenzado a plantear un concepto aún más amplio, conocido como *finanzas abiertas*, que engloba una democratización mayor a la planteada en la UE. Este concepto incluye la posibilidad de participación de nuevos



agentes en sectores como créditos, seguros o inversión<sup>10</sup>. Estas propuestas sugieren requerimientos regulatorios más livianos en función de la criticidad de la actividad, mediante nuevas licencias o simples registros. Esto ha permitido que estos países se conviertan en los primeros en adoptar la innovación tecnológico-financiera.

De esa manera, se produjo un salto de los países emergentes, en el cual se pasa de un estándar operativo cerrado propio de la etapa *FinTech 2.0* a un modelo que abarca no solo la apertura e innovación en el procesamiento de datos financieros por parte de nuevos agentes en el campo de los pagos, sino también en todos los ámbitos financieros, incluyendo la inversión y los seguros.

Por esta razón, en el mismo periodo se creó una divergencia entre la UE y los países emergentes. En ambos casos, el elemento común es que tanto la banca abierta (centrada en los pagos y propia de la UE) como las finanzas abiertas (apertura en todos los ámbitos financieros y propia de los países emergentes) continúan regulándose con base en la existencia de un banco central emisor de dinero de curso legal y una red de entidades legales con capacidad para ofrecer servicios financieros. Es decir, la figura del tercero de confianza sigue presente y está definida por una entidad legal, siendo un requisito indispensable para el desarrollo de la actividad. En ese sentido, la necesidad de confianza social se mantiene, puesto que se confía en un tercero (regulado o no) y en sus afirmaciones para identificar lo que poseemos, lo que nos deben y lo que debemos (*what we own, what we're owed, and what we owe*) (Casey y Vigna, 2018, pp. 1-10). La aparición de nuevos agentes centralizados en los que confiar es lo que hace que se pueda catalogar esta etapa como *CeDeFI*.

A estos efectos, para abarcar estos fenómenos paralelos en el tiempo, el avance de la banca abierta liderada en UE se consideró como *FinTech 3.0* y el avance de finanzas abiertas liderado por los países emergentes se denominó *FinTech 3.5*. En lo concerniente al desacople entre los nuevos modelos *FinTech* y la normativa existente, se debe tener en cuenta que los nuevos arquetipos de negocio antes delineados son exclusivos de países emergentes. Es decir, ha habido un surgimiento de nuevas actividades *FinTech* en áreas como préstamos, seguros, inversión y otros, que actualmente no cuentan con marcos normativos actualizados en la UE, lo que genera una situación de alegalidad como se mencionó anteriormente.

---

<sup>10</sup> Ejemplos de iniciativas de *open finance* son Brasil, Chile o Colombia (Open Banking Brasil, 2021)

Simplemente, cabe señalar que han surgido nuevos patrones o modelos híbridos en los que resulta difícil determinar dónde termina un servicio tecnológico y comienza un servicio financiero sujeto a regulación. Estos modelos se intensifican en el caso de las denominadas *BigTech* o *TechFin*. Por este motivo, es necesario hacer una distinción entre servicios puramente tecnológicos de apoyo a la actividad financiera, que están cubiertos por la normativa existente, y aquellos servicios financieros innovadores que requieren una nueva regulación marco (esto se aplica a la regulación de plataformas de financiación participativa o criptoactivos).

No solo eso, sino que las tecnologías también han llevado a una redefinición de roles, lo que ha llevado a actores no regulados o semi-regulados a realizar actividades que originariamente estaban reservadas para la banca. Si bien la Segunda Directiva de Pagos contempla una apertura en términos de transacciones en cuentas corrientes (proveedores de servicios de pago e iniciadores de pagos), en las finanzas abiertas esta apertura de actividades se extiende más allá hacia las actividades financieras en general. Por lo tanto, se están replanteando los límites de las actividades bancarias reservadas. El extremo se alcanza con las DeFi y las criptomonedas, donde incluso la emisión de valor, que tradicionalmente estaba asignada a los bancos centrales, ahora tiene competidores en el sector privado (las *stablecoins*).

Como resultado de estos desacoples, los modelos de supervisión se han visto impactados, precisando de nuevas soluciones flexibles como los *sandboxes* regulatorios, que se evaluarán en capítulos posteriores. Estos *sandboxes* no solo representan una nueva forma experimental de supervisión, sino también una manera de detectar lagunas regulatorias o desajustes entre los requisitos y las nuevas realidades.

## **2. Los agentes**

Las etapas *FinTech* 3.0 y 3.5 se caracterizan por la aparición de nuevos agentes en el lado de la oferta de servicios financieros. Si bien estos agentes surgen en esta etapa, al igual que la banca, continúan participando en distintos roles a lo largo de *FinTech* 4.0, adoptando modelos híbridos en los que se ofertan servicios relacionados con criptoactivos, pero de manera centralizada.

Atendiendo a su origen, se pueden identificar tres grupos de entidades involucradas en el fenómeno *FinTech*: entidades de pequeño tamaño (*start-ups*), entidades de origen en grandes grupos tecnológicos, redes sociales y plataformas (*BigTech*) y entidades

financieras (*incumbents*). Esta clasificación no es específica de la UE, sino que, debido a que estos modelos tienen una finalidad de atención al cliente global, se clasifican generalmente así independientemente de la jurisdicción en que operan. Es más, varios de estos agentes operan de manera externa, ofreciendo servicios transfronterizos.

Debido a la falta de claridad jurídica, estos modelos pueden tender a establecerse en zonas de bajos o nulos requerimientos regulatorios respecto a la actividad desarrollada, dando lugar a los denominados “arbitrajes regulatorios”. Esto se da específicamente en los casos de *FinTech start-up* y *TechFin*.

A continuación, se identifican los principales agentes en *FinTech* 3.0 y 3.5, los cuales son uno de los componentes por los que se puede defender la argumentación de que estas fases ya pueden considerarse como disruptivas. Si bien las etapas *FinTech* 1.0 y 2.0 contaban con las entidades financieras (*incumbents*) para implementar la innovación en finanzas, en *FinTech* 3.0 y 3.5 se abren las puertas a nuevos agentes que a su vez impulsan la innovación tecnológica. Estos agentes son las *FinTech start-up* y las *TechFin* (*BigTech*).

## **2.1 *FinTech start-up***

Las *FinTech start-ups* son pequeñas empresas dedicadas a la actividad financiero-tecnológica. Su tamaño les permite funcionar de una forma más ágil que la banca tradicional. Suelen especializarse en determinados nichos o puntos de la cadena de valor de pagos, optimizando su modelo de negocio mediante el empleo de nuevas tecnologías y altos niveles de automatización con el fin de alcanzar economías de escala una vez aumenten de tamaño.

Por lo general, las *FinTech start-ups* tiene como objetivo salir a bolsa o ser adquiridas por entidades de gran tamaño. Por este motivo, pasan por diversas etapas de crecimiento que regularmente van financiadas por distintas rondas de inversión y perfiles de inversores (familiares y amigos, aceleradoras, ángeles inversores y fondos de capital riesgo). El paso de una etapa a otra depende del nivel de crecimiento y alcance de distintos hitos que la *start-up* debe demostrar antes de pasar a las siguientes rondas de inversión. En la etapa inicial (pre-semilla, preserie A), existe un mayor riesgo de desaparición si no se valida la idea de negocio y, por tanto, se da una mayor inestabilidad de la *FinTech*.

Las *FinTech* pueden estar reguladas o no en función de la actividad que realizan y el país en el que se encuentran. En concreto, en la UE pueden estar reguladas bajo una normativa europea, una normativa sectorial específica, una regulación local o no estar reguladas (European Banking Authority [EBA], 2017a, p. 9). A modo de ejemplo, un estudio de la European Banking Authority (EBA) de 2017 mostró que un 31 % de las *FinTech* de los Estados Miembros no estaban reguladas (European Banking Authority [EBA], 2017b, p.21). Si operan como intermediarios tecnológicos o tienen contacto con el público, generalmente se centran en ofrecer mejores experiencias de usuario, reduciendo fricciones habituales que estos suelen encontrarse en las interacciones de tipo financiero (por ejemplo, tener que desplazarse a una oficina o realizar operaciones manuales o repetitivas).

Este tipo de entidades a menudo buscan cómo combinar los conceptos de finanzas e innovación con proyectos de responsabilidad social corporativa o *Environmental, Social and Governance* (ESG), como pueden ser de tipo social o medioambiental. Entre las nuevas ideas relacionadas con el medioambiente, cabe mencionar la asociación de pagos con la huella de carbono derivada de la transacción realizada (Muhn, 2021, pp. 1-3).

Las entidades *FinTech* dirigen su actividad a una categoría diferente de clientes. Su opción suele ser la de atender a colectivos desatendidos por la banca tradicional, es decir, poblaciones no bancarizadas o sub-bancarizadas. Las *FinTech* son expertas en la captación y gestión de los datos, por lo que introducen innovaciones en el modelo de negocio, dado que, al dirigirse a sus clientes, incluyen tácticas predictivas para conocer mejor sus necesidades y capacidad de cumplimiento de obligaciones de pago. Esta característica es compartida con los siguientes sujetos de estudio, las *TechFin*.

## **2.2 *TechFin* (BigTechs)**

Si bien las *FinTech start-ups* parten desde cero y tienen el desafío de demostrar su capacidad de crecimiento basándose en clientes, las *TechFin* comienzan su trayectoria en el mundo financiero partiendo de una masa crítica de clientes potenciales que ya confían en sus productos (Tanda y Schena, 2019, pp. 37-49).

Las *TechFin* se caracterizan por tener su origen en el mundo digital no regulado (tecnología, plataformas, redes sociales o entretenimiento). Es por este motivo que cuentan con datos de los clientes que los bancos tradicionales no tienen. Además, conocen mejor a su público objetivo, puesto que llevan empleando herramientas de analítica de

datos y predicción del comportamiento desde hace mucho más tiempo (Adrian, 2021, pp. 1-3). En otras palabras, comienzan con los datos y la oferta de servicios financieros se vuelve un paso natural para optimizarlos (Zetsche et al., 2017, p.9).

Estas entidades cuentan con un músculo financiero incluso mayor que los de la propia banca comercial. En 2018, los niveles de capitalización de varias de estas entidades eran incluso mayores que los de los bancos más grandes del mundo como JP Morgan, ICBC, Bank of America, Wells Fargo, China Construction Bank, HSBC o Ant Financial (Carstens, 2018) (ver Figura 4 ).

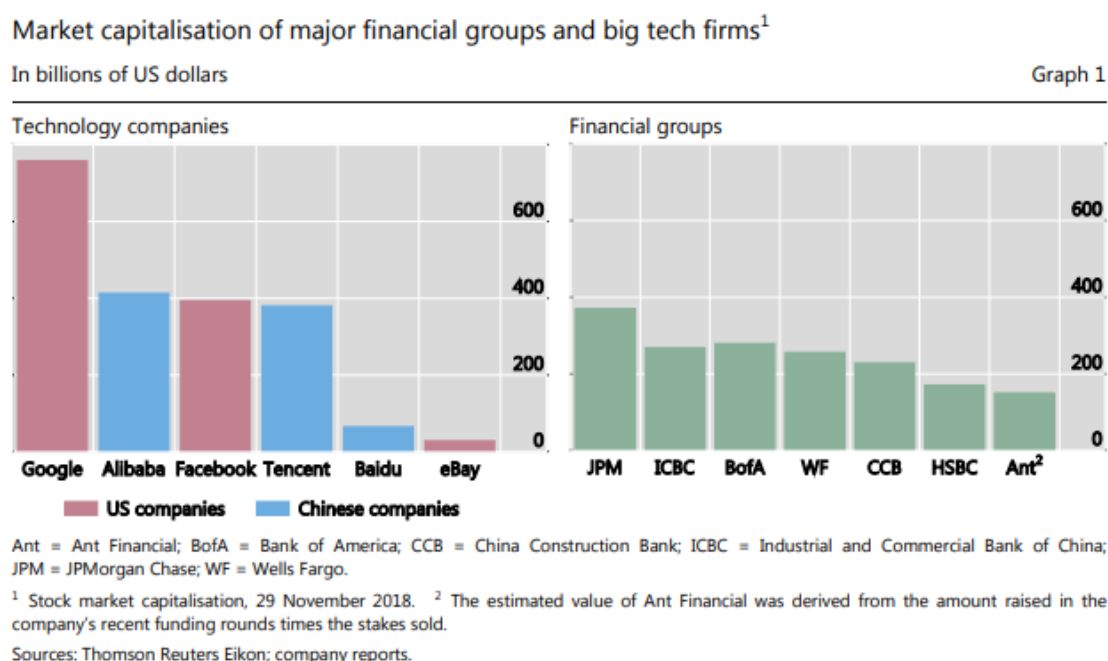


Figura 4. Capitalización de BigTech versus los mayores grupos financieros

Nota. Tomado de *Big tech in finance and new challenges for public policy*, por A. Carstens, <https://www.bis.org/speeches/sp181205.htm>

Las primeras *TechFin* que iniciaron su incursión en el mundo financiero occidental fueron Google, Amazon, Facebook y Apple (conocidas como GAFAM). A estas entidades se suman otras como Microsoft, Uber o eBay. Su estrategia se ha centrado en comenzar su entrada en el mundo financiero mediante colaboraciones con entidades financieras (*incumbents*) para posteriormente desarrollar sus propios negocios financieros, generalmente a partir de servicios de pagos (billeteras digitales).

En la zona asiática, Baidu, Alibaba, Tencent y Xiaomi (conocidas como BATX) adoptaron estrategias de desarrollo de entidades con licencia propia, creando sus propios verticales de pagos. A estas *FinTech* asiáticas de primera generación se han sumado

entidades como NTT DoCoMo y Rakuten (Japón), Samsung (Corea del Sur) y Grab (Singapur) (Carstens, 2018). En la UE, esta evolución se ha visto principalmente en *BigTechs* relacionadas con el sector de telecomunicaciones (Orange y Vodafone), mientras que en América Latina las empresas de plataformas, principalmente *e-commerce*, movilidad y servicio a domicilio, son las que han tomado este enfoque de diversificación hacia el mundo financiero (Mercado Libre<sup>11</sup> y Rappi<sup>12</sup>, entre otros).

Las ventajas competitivas con las que parten dependen del subsector al que pertenezcan. Por ejemplo, las plataformas de comercio electrónico y las redes sociales pueden contar con una mayor cantidad de datos que les permiten perfilar mejor a sus clientes. Además, sus usuarios son nativos digitales que están acostumbrados a utilizar aplicaciones de forma recurrente. Por otro lado, los usuarios de servicios de telecomunicaciones no necesariamente son nativos digitales y tienen menos tráfico recurrente en sus sitios web o aplicaciones.

Si bien los datos y su novedoso tratamiento también son una ventaja identificada en las *FinTech*, estas, debido a su estado embrionario, no cuentan con una base de clientes equiparable a las de las *BigTech*. Debido a la gran diferencia de clientes (pudiendo tratarse de *BigTech* globales o que cubren grandes regiones), los datos generados por los usuarios de estas empresas tienen un carácter exponencial que permite el desarrollo de mejores herramientas de predicción de comportamientos y preferencias. Es decir, el tratamiento a través de la innovación es similar al caso *FinTech*; sin embargo, la capacidad de volúmenes de datos generados y el recorrido de captura temporal de estos no tiene comparación entre unos y otros.

Sumado a lo anterior, la capacidad de apalancarse sobre la experiencia obtenida en otras industrias a lo largo de los años por parte de las *BigTech* es uno de los principales motivos de preocupación de las autoridades, quienes estiman que estos conglomerados podrían ir más allá de sus mandatos y jurisdicciones, sin ser capaces de evaluar el impacto total (*end-to-end*) de las actividades financieras de las *BigTech* (Bank of International Settlements [BIS], 2019, pp. 1-26). A modo de ejemplo, Estados Unidos elaboró un borrador de regulación que prohibía la posibilidad de que empresas tecnológicas de gran tamaño se dedicasen a la oferta de servicios financieros o adquirieran entidades

---

<sup>11</sup> Mercado Libre es un grupo dedicado al comercio electrónico que ha desarrollado su propio brazo financiero, llamado Mercado Pago (Mercado Libre, 2021).

<sup>12</sup> Rappi es una plataforma colombiana de servicio de comida a domicilio presente en varios países de América Latina (Crunchbase, 2021c).

financieras reguladas (Senate and House of Representatives of the United States of America, 2019, pp. 2-7). Las *BigTech* se abordan en profundidad como los sujetos de principal calado en *FinTech* 3.5.

### **2.3 Entidades financieras (incumbents)**

Las entidades financieras relacionadas con el mundo de los pagos (principalmente entidades de crédito y emisoras de dinero electrónico) se han visto obligadas a replantear sus estrategias debido a (i) cambios regulatorios (iniciativas de banca abierta como PSD II), (ii) la entrada de nuevas contrapartes (*FinTech start-up* y *BigTechs*), (iii) la disrupción de nuevas tecnologías y (iv) los cambios en las expectativas de los usuarios (European Banking Authority [EBA], 2019b, pp. 10-14).

Las reacciones ante el fenómeno *FinTech* varían entre las instituciones financieras. La opción más común en la zona europea ha sido el lanzamiento de proyectos internos de digitalización (European Banking Authority [EBA], 2019b, pp. 6-34). En casos donde existía una falta de conocimiento interno, dificultades debido a infraestructuras de sistemas arcaicas o la necesidad de acceso a nuevos servicios o colectivos, la colaboración con *FinTech* se vuelve más frecuente (Tanda y Schena, 2019, pp. 10-49). Los usos más extendidos son el desarrollo de frontales tecnológicos para mejorar la experiencia del usuario, soluciones de *back office* (automatizaciones, capas de interfaces de programación de aplicaciones) y soluciones de mejora de obligaciones regulatorias (*RegTech*) (European Banking Authority [EBA], 2019b, pp. 6-34).

También se han producido adquisiciones de *FinTech*, pero en menor medida, puesto que principalmente solo los grandes bancos pueden permitirse inversiones de este tipo (European Banking Authority [EBA], 2019b, p. 15). En el supuesto de interacción con las *BigTech*, a menudo se combina la colaboración con el hecho de que estas entidades ya eran proveedoras de los bancos (por ejemplo, los bancos que utilizan servicios de la nube de Amazon, AWS). Sin embargo, el creciente interés de las *BigTech* en los servicios financieros también se percibe como una amenaza de entrada de competidores con un gran impacto en el sector bancario.

Estas estrategias de interacción con las *FinTech* y *BigTech* es solo una parte del replanteamiento global que la banca deberá llevar a cabo en los próximos años. Deloitte, en su informe *Swiss Banking Business Models of the Future*, señaló cinco modelos de

negocio que los bancos podrán adoptar (Deloitte Consulting A.G., 2015, pp. 3-43) (ver Figura 5):

El primer tipo de perfil sería el del campeón de transacciones (*transaction champion*). Bajo este perfil, los bancos trabajarían como un operador transaccional de otros bancos o de *FinTechs*.

La segunda opción sería la de líder de producto (*producto leader*), por el cual la entidad financiera se centraría en una oferta de productos y servicios innovadores.

La tercera opción de línea de trabajo sería la del asesor de confianza (*trusted advisor*). En este caso, el banco estaría enfocado en los clientes, ofertando servicios adaptados a sus necesidades y asesorando sobre ellos.

El cuarto tipo de banco sería el del proveedor de soluciones administrativas (*managed solutions*). Estas instituciones tendrían una oferta de servicios de soporte a los anteriores modelos (operarían como un *back office* del resto de servicios).

Finalmente, el banco universal (*universal bank*). Este modelo necesitará de una mejora en eficiencia con respecto a la actualidad, debido a la futura reducción de márgenes en la banca.

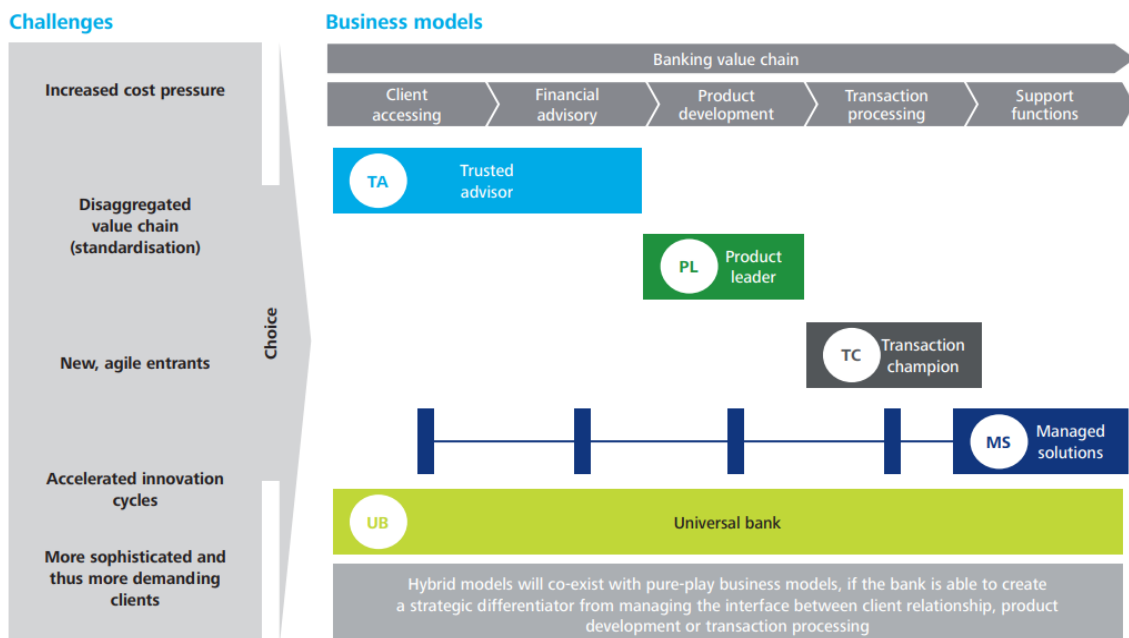


Figura 5. Futuros modelos de negocio de la banca

Nota. Tomado de Swiss Banking Models of the Future. Embarking to New Horizons, por Deloitte Consulting A.G., 2015, <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/financial-services/ch-en-fs-bank-of-tomorrow.pdf>.



## 2.4 Comparativa

Cada uno de estos tres grupos gozan de ventajas competitivas, riesgos e inconvenientes, como se resume en la Tabla 2.

Concepto	<i>FinTech start-up</i>	<i>TechFin (BigTech)</i>	Entidades financieras
Masa crítica de clientes	Baja	Alta	Alta
Confianza de clientes	Baja	Alta	Alta
Experiencia de usuario	Alta	Alta	Media
Inmediatez	Alta	Alta	Media
Inclusión financiera como objetivo	Alta	Baja	Baja
Productos adaptados a la necesidad del cliente	Alta	Alta	Media
Explotación y optimización de datos	Alta	Alta	Media
Adecuada gobernanza de datos	Baja	Media	Alta
Flexibilidad, agilidad de cambio	Alta	Alta	Baja
Uso de nuevas tecnologías	Alta	Alta	Baja
Solvencia financiera	Baja	Alta	Alta
Estabilidad del modelo de negocio	Baja	Alta	Alta
Seguridad regulatoria	Baja	Media	Alta
Cultura de cumplimiento	Baja	Baja	Alta
Nivel de supervisión	Baja	Media	Alta
Riesgo tecnológico	Alto	Alto	Alto
Riesgo de tercerización ( <i>outsourcing</i> )	Alto	Medio	Medio

Tabla 2. Análisis comparativo *FinTech start-up*, *TechFin* y entidades financieras

Nota. Elaboración propia.

Como se observa en la Tabla 2, las *FinTech start-ups* tienen ventajas similares a las *BigTech* en términos de experiencia de usuario, inmediatez y oferta de productos adaptados. Esto se complementa con una nueva forma de explotación y optimización de los datos compartidos o generados de los clientes mediante el uso de nuevas tecnologías. Sin embargo, las *FinTech* se diferencian de las *TechFin* en que las primeras no son negocios inicialmente solventes o estables y su nivel de supervisión y regulación es bajo, por lo que son más débiles, y suelen acudir a soluciones externas para elementos operativos.

Por otro lado, tanto las *BigTech* como las entidades financieras gozan de una estabilidad en modelo de negocio y solvencia, así como una amplia base de clientes. Sin embargo, las *BigTech* explotan los vacíos regulatorios existentes en la actualidad y, en numerosas ocasiones, han recibido críticas por sus bajos niveles de cumplimiento.

Las *FinTech* y *BigTech* pueden relacionarse con los *incumbents* de distintas formas: (i) como competidores directos, entrando a ofrecer los mismos productos y servicios a colectivos ya atendidos por las entidades financieras; (ii) como competidores adyacentes,

cubriendo una oferta de productos y servicios nuevos que las entidades financieras tendrían el potencial de cubrir, pero que no lo han hecho hasta ahora (la pérdida sería en términos de coste de oportunidad); (iii) el tercer y último caso comprende los modelos de colaboración o facilitadores, en los que los nuevos participantes entran en modelos de colaboración y generación de sinergias (Hauptman, y otros, 2022, pp. 4-5).

Una vez conocidos los agentes comunes a las etapas 3.0 y 3.5, a continuación, se analizan los modelos *FinTech* 3.0 centrados en pagos, distinguiendo entre los impactos relacionados con la clientela y aquellas innovaciones de las propias infraestructuras de pagos.

## **II. FINTECH 3.0: LA BANCA ABIERTA EN EUROPA**

### **1. Planteamiento**

No cabe duda de que el sector *FinTech* está en constante evolución. Indicio de ello es la proliferación de la regulación europea en los últimos años en torno a las innovaciones de carácter tecnológico-financiero.

La Primera Directiva de Servicios de Pago<sup>13</sup> (PSD I) de 2007 supuso un gran avance en Europa, al plantear una homogeneización de los pagos en toda la zona euro. En palabras de Tapia Hermida, “sentó las bases jurídicas de la creación de un mercado único de servicios de pago en toda la UE” (Tapia, 2018, p.18). De esta manera, se mejoraron las condiciones de acceso y uso de los servicios de pago en la región, incentivando una adecuada competencia y reduciendo las barreras existentes en términos de actividad limitada por las jurisdicciones. De esa manera, a través de los cambios normativos se promovió un modelo de banca abierta u *open banking*, siendo los servicios de pago su campo de pruebas. El objetivo de la implementación de la banca abierta era aumentar el flujo financiero del mundo analógico hacia un entorno digital más competitivo, donde se permitieran nuevos participantes y se erosionaran las barreras de entrada de las que disfrutaba la banca tradicional (Muñoz, 2021, pp. 2-3).

Sin embargo, esta normativa quedó rápidamente desactualizada debido a los cambios tecnológicos producidos en la fase *FinTech* 3.0, lo que llevó a la necesidad de desarrollar

---

<sup>13</sup> Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE.

nuevas regulaciones. Estas necesidades regulatorias ya las había identificado la Comisión Europea (CE) en 2013 en su informe titulado *Report from the Commission to the European parliament and the Council on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation (EC) No 924/2009 on cross-border payments in the Community*.

En dicho documento se expuso la necesidad de un nuevo desarrollo normativo con la finalidad de promover la libre competencia y tener en cuenta los nuevos avances tecnológicos que se habían producido ya en el periodo de tiempo entre su publicación y el análisis. En efecto, era evidente la necesidad de ampliar el ámbito de aplicación, puesto que la primera directiva solo aplicaba a los proveedores de servicios de pago (PSP) por ambas partes (ordenante y receptor) cuando se encontraban en el espacio económico europeo. Además, PSD I había excluido ciertas actividades que habían ido ganando peso en el mercado (por ejemplo, el servicio de información de cuentas o de iniciación de pagos), por lo que su uso por parte de los consumidores quedaba fuera de protección.

La CE también especificó que era necesaria la revisión debido a la aparición de empresas que ofrecían servicios de pago de corte tecnológico:

*Es necesario también dar cabida a la evolución tecnológica de las empresas. Han aparecido en el mercado nuevos operadores («proveedores de servicios de pago terceros»), que ofrecen básicamente soluciones de pago de bajo coste en internet, utilizando la aplicación de banca en línea de que disponen en su domicilio los clientes, con el consentimiento de estos, e informando a los comerciantes de que el dinero está en camino, de tal forma que facilitan las compras en línea. Algunos operadores también ofrecen información agregada sobre diferentes cuentas de un usuario de servicios de pago («servicios de información sobre cuentas»). Aunque estos nuevos agentes suponen ventajas indiscutibles para los usuarios de servicios de pago en general –tanto los comerciantes como los consumidores– y para la competencia en el mercado, es necesario aportar una respuesta a nivel de la UE a una serie de cuestiones que se plantean en lo que respecta a la seguridad, el acceso a la información sobre las cuentas de pago o la privacidad de los datos, así como a su posible autorización y supervisión como entidades de pago en virtud de la DSP<sup>14</sup>. (Comisión Europea, 2013, pp. 2-10)*

---

<sup>14</sup> DSP hace referencia a la Directiva de Servicios de Pago.

En ese sentido, la apertura a la innovación en el entorno de pagos fue producto de la iniciativa europea de banca abierta, que se cristalizó en 2015 mediante la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior. Esta regulación dio respuesta a las críticas que la CE hizo en 2013 y permitió abrir los datos de pagos a terceras partes mediante el uso de la tecnología.

En el ámbito local, esta directiva se transpuso a través del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y el Real Decreto 736/2019, de 20 de diciembre, de régimen jurídico de los servicios de pago y de las entidades de pago. Sin embargo, la normativa solo hace referencia a cierto tipo de servicios de pagos, siendo el universo de las actividades *PayTech* (tecnología de pagos) más amplio. Por este motivo, es importante establecer qué son actividades y modelos de negocios *PayTech*, así como estudiar las entidades que lo conforman y la necesidad o no de regular todo este ecosistema. *PayTech* supone un giro en pagos que se refleja en dos aspectos fundamentales que a continuación se identifican y que estructuran la totalidad del presente capítulo: la revolución en las entidades intervinientes y la revolución en las infraestructuras.

### ***1.1 Revolución en las entidades intervinientes***

Esta sección realiza un análisis del panorama actual de las *FinTech* de pagos (*PayTech*) en la UE, describiendo su actividad y las innovaciones tecnológicas que, por lo general, aplican. Posteriormente, se evalúan las problemáticas a las que se enfrentan en la actualidad, proponiendo puntos de mejora de los marcos regulatorios existentes.

Cabe mencionar que en este estudio se deja fuera de ámbito el análisis del ecosistema de proveedores de servicios de criptoactivos, que se abordan separadamente.

### ***1.2 Revolución en las infraestructuras***

La apertura a la innovación en las infraestructuras de pagos ha supuesto un cambio no solo a nivel europeo, sino también a nivel global. Por este motivo, se dedica una sección dentro del ámbito de *FinTech* 3.0. Esta sección se aborda desde la perspectiva de las iniciativas y retos que se están viendo a nivel global para poder dar un alcance completo a la cuestión. De esa manera, se lleva a cabo un estudio de las decisiones tomadas por el *Bank of International Settlements* (BIS).

## 2. Aproximación a las *PayTech*

Las entidades *FinTech* de pagos digitales o *PayTech* se definen como “cualquier compañía que, apoyándose en la tecnología, desarrolla soluciones de pago innovadoras que mejoran las características y capacidades de los medios de pago existentes, y proveen una mejor experiencia de usuario” (Asociación Española de *FinTech* e *InsurTech* [AEFI], 2020, p. 1).

El término *PayTech* surgió de la combinación de los términos *payment* (pago en inglés) y *technology* (tecnología), haciendo alusión a la tecnología en pagos, siguiendo el modelo del término *FinTech* (tecnología en finanzas). Si se tiene en cuenta la definición que el *Financial Stability Board* (FSB) hizo sobre el concepto de *FinTech* en general, y acotándolo al entorno de pagos, se podría dar luz a una definición más amplia a la anterior: el uso de la innovación habilitada por la tecnología en los servicios financieros que podría resultar en nuevos modelos de negocio, aplicaciones, procesos o productos (relacionados con pagos), y podría tener un efecto material asociado sobre las finanzas, mercados e instituciones y cómo se proporcionan los servicios (de pagos) (Financial Stability Board [FSB], 2021, p. 1). De este modo, se cubrirían no solo las empresas, sino también cualquier innovación con impacto en pagos, incluyendo las propias infraestructuras que los soportan.

Los pagos son un elemento más del día a día de cualquier persona. Si se trasladara la pirámide de Maslow (1954) al entorno del mundo financiero y se tuvieran que fijar prioridades, podría concluirse que las necesidades financieras de las personas deben graduarse de mayor a menor, tomando como base la necesidad de tener cuentas, realizar pagos y tener acceso a créditos. En un segundo nivel estaría la capacidad de acceder a seguros médicos y planes de pensiones. El tercer nivel sería para otro tipo de seguros y, finalmente, la cúspide de la pirámide se asignaría a los productos de inversión y optimización de la gestión de patrimonio. El subir escalones de dicha pirámide dependería del poder adquisitivo o la capacidad de ahorro que vayan adquiriendo las familias (ver Figura 6).

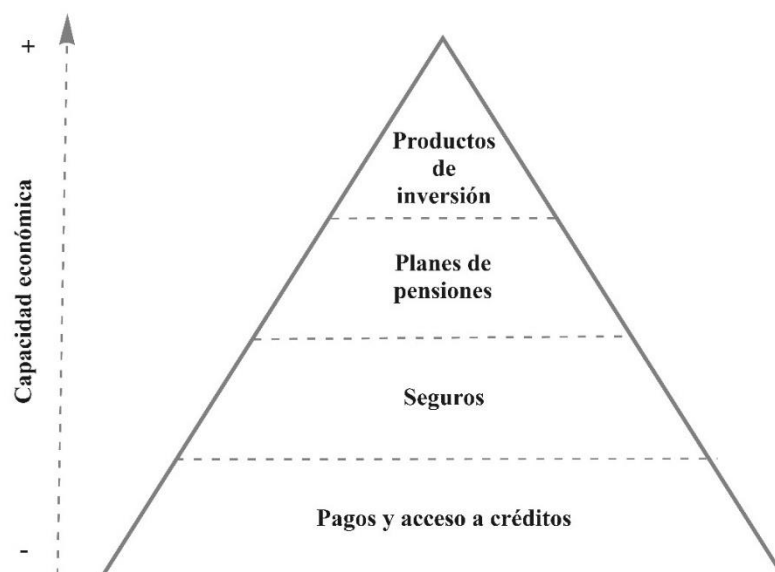


Figura 6. *Pirámide de necesidades económicas*

Nota. Elaboración propia

Es precisamente el sector de pagos el que actualmente está experimentando grandes cambios, tanto desde el punto de vista estructural (mejoras o propuestas de nuevos canales de pagos) como en el modelo de oferta al público, siendo este último el objeto de este estudio.

La proliferación de la industria *PayTech* ha sido favorecida por elementos regulatorios, tecnológicos y coyunturales. Como se indicó anteriormente, la Directiva conocida como PSD II (Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) 1093/2010 y se deroga la Directiva 2007/64/CE, 2015) sentó las bases del concepto de *banca abierta en pagos*. Dicha directiva se basaba en la tecnología de interfaces de programación (denominadas API) abiertas entre entidades financieras y terceros para el intercambio de datos de acuerdo con los protocolos de seguridad adecuados. Además, la crisis de la COVID-19 impulsó soluciones de pagos digitales en diferentes regiones, como Europa con pagos a través de teléfonos inteligentes, y otros países como China, India o México con pagos mediante QR<sup>15</sup> o NFC<sup>16</sup>. También ha fomentado la digitalización de

<sup>15</sup> *Quick response* o QR hace referencia a un código de respuesta rápida. Según la organización de consumidores y usuarios, es una etiqueta óptica que contiene información y puede ser leída por una máquina (Organización de Consumidores y Usuarios [OCU], 2022).

<sup>16</sup> Según el Banco de México, la tecnología NFC (comunicación de campo cercano) se basa en la transmisión de datos e información, con el solo hecho de aproximar dos dispositivos móviles entre sí.

los servicios asociados a los pagos, como la apertura de cuentas completamente digitales, el uso de validación biométrica y la implementación de técnicas de aprendizaje automático para mejorar la detección de fraudes.

El apoyo de las administraciones públicas en favor del impulso en la innovación también ha jugado un papel importante en la proliferación de estas instituciones. A modo de ejemplo, en la zona euro, el gobierno sueco ha apoyado la iniciativa de la asociación de bancos de implantación, esto es, un sistema de identidad digital denominado bankID (BankID, 2021, p.1). Fuera de la zona europea, países como India, China o Singapur han desarrollado soluciones similares. Recientemente, la UE publicó un documento de consulta en este mismo sentido con el fin de plantear una identidad digital soberana a través de eIDAS 2<sup>17</sup>.

### **3. Los sujetos. Criterios de clasificación de las *PayTech***

Bajo el propio término de *PayTech* se pueden identificar distintos tipos de entidades que pueden clasificarse de diferentes maneras en función de su origen, licencias bajo las que operan y rol o actividad a la que se dedican. A continuación, se expone cada uno de ellos.

#### ***3.1 Taxonomía en función del tipo de licencias***

Como se mencionó anteriormente, las *FinTech* de pagos pueden contar con distintos rangos de licencias e incluso en caso de ciertos servicios auxiliares. De ser así, las entidades operarían como meros proveedores tecnológicos.

Cabe elaborar una enumeración de los distintos tipos de entidades *PayTech* según el criterio de las licencias con las que cuentan. En una escala de menor a mayor, el primer grupo serían los denominados proveedores tecnológicos. Bajo este concepto se agrupan todas las entidades de servicios tecnológicos no supervisados, que por lo general suelen aludir a proveedores de capas de servicios API o entidades de servicios auxiliares a pagos (por ejemplo, herramientas de monitorización de operaciones o prevención de fraude, seguridad o servicios post pago) (AEFI, 2020, pp. 37-38).

---

<sup>17</sup> eIDAS 2: Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea COM/2021/281 final.

En un segundo escalón se encontrarían las *PayTech* con licencias limitadas que suelen especializarse en ciertos segmentos de la cadena de valor (iniciación de pagos, servicios de agregación o emisión de dinero electrónico). En consecuencia, estas entidades necesitan integrarse con entidades financieras para acceder a las infraestructuras de pago y cámaras de compensación y liquidación.

El tercer nivel lo ocuparían los denominados neobancos. A este respecto, existen discrepancias en torno a la definición del concepto de *neobancos*. Algunas instituciones equiparan el concepto de *neobancos* con el de *challenger banks*, implicando una licencia bancaria. Sin embargo, en la práctica se emplea esta acepción para referirse a *PayTech* de licencias limitadas o sin licencia propia que se apalancan en terceros (González de Audinaca, 2019), reduciendo sus costos y tiempo de entrada al mercado, al tiempo que ofrecen otro tipo de servicios complementarios a sus usuarios, resultando en una aplicación o web cuya apariencia es similar a la de un banco debido a la variedad de productos que se ofertan, siendo parte propios y parte locales. Los neobancos son grandes consumidores de los nuevos modelos contractuales derivados de la banca abierta: *Banking as a Service* (BaaS) o *FinTech as a Service* (FaaS). Se caracterizan por enfocarse en clientes individuales, emprendedores y pequeñas y medianas empresas (pymes) (Basel Committee on Banking Supervision and Bank of International Settlements, 2018, p. 18).

Los *challenger banks* son *PayTech* con licencias bancarias y operan 100 % de manera digital. Estos bancos se enfocan en la experiencia del usuario, pudiendo “personalizar su uso, con el fin de general valor en el mercado, con nuevas propuestas de precios, productos y servicios” (González de Audinaca, 2019, p.1). Su origen puede ser *FinTech start-ups*, como es el caso de Revolut<sup>18</sup>, Monzo<sup>19</sup> o Starling Bank<sup>20</sup>, pero también existen casos de *challenger banks* producto de *BigTech*, como puede ser Orange Bank. Estos segundos escenarios suelen ser más habituales en la zona asiática, debido a la existencia de licencias bancarias digitales específicas y a las estrategias tomadas por las *BigTech* de esos países.

Todo este tipo de nuevas partes en torno a *PayTech* se caracterizan por carecer de presencia física, ahorrando costos con respecto a la banca tradicional. Tampoco cuentan

---

<sup>18</sup> Revolut obtuvo su licencia en diciembre de 2018 (Singapore Fintech Association y BCG, 2020).

<sup>19</sup> Monzo obtuvo su licencia en abril de 2017 (Singapore Fintech Association y BCG, 2020).

<sup>20</sup> Starling Bank obtuvo su licencia en julio de 2016 (Singapore Fintech Association y BCG, 2020).



con herencias técnicas (sus sistemas son de última generación). Asimismo, sus operaciones y sistemas están en la nube, permitiendo economías de escala.

En la actualidad, el foco de debate respecto a este tipo de clasificación está en hasta dónde han de cubrir los supervisores financieros, es decir, dónde acaba la parte financiera de la actividad *FinTech* y dónde comienzan los servicios no regulados, puesto que los límites entre uno y otro cada vez son más difusos. Hasta el momento, se ha apelado a aplicar el principio de “misma actividad, mismo riesgo, misma regulación” (Restoy, 2021, pp. 5-22). Sin embargo, este principio cada vez se hace más complejo debido a la deslocalización y fragmentación de las cadenas de valor de pagos y servicios asociados (Comisión Europea, 2021d, pp. 1-13). Además, a menudo entidades reguladas llegan a tener alta dependencia de las no reguladas, por lo que su impacto operacional puede provocar alteraciones en el mundo financiero.

### **3.2 Según su actividad**

La propuesta de la Asociación Española de *FinTech* e *InsurTech* consiste en organizar la estructura de verticales *PayTech* y englobar este tipo de *FinTechs* en tres grandes grupos de emisoras, adquirentes y otras, siempre teniendo en cuenta que distintas *FinTech* pueden realizar actividades pertenecientes a más de un grupo.

#### **3.2.1. *FinTech* emisoras**

Las *FinTech* emisoras son aquellas entidades cuyas funciones consisten en “emitir y/o proporcionar un instrumento de pago por parte del proveedor al PSU (usuario de servicios de pago) final” (Asociación Española de *FinTech* e *InsurTech*, 2020, pp. 24-25). Una de las principales novedades de la aplicación de innovaciones en la emisión de instrumentos de pago ha sido el desarrollo de soluciones tecnológicas que permiten la emisión de tarjetas virtuales que se pueden emplear prácticamente desde el momento en el que el usuario abre una cuenta. En virtud de ello, se habla de soluciones de emisión instantánea (AEFI, 2020, pp. 24-63). De este modo, se reducen drásticamente los tiempos de espera para la creación y entrega de las tarjetas físicas. Además, cada vez más se ofrece la posibilidad de la simple emisión de las tarjetas virtuales, dejando a la opción del cliente la solicitud de la tarjeta física e incluso repercutiendo los costos de esta.

Una evolución ulterior se representa mediante las denominadas tarjetas virtuales *tokenizadas* que permiten guardar fondos en billeteras digitales (Apple Pay, Samsung

Pay, entre otras). La tecnología *contactless* facilita que puedan utilizarse tan solo acercando el teléfono a los terminales (AEFI, p. 23). La mencionada *tokenización* cobra fuerza porque añade niveles de seguridad de los datos de tarjetas. El robo de datos es uno de los principales riesgos que han aflorado con el uso de nuevas tecnologías y es frecuente ver noticias de prensa referidas a robo de datos masivos y puesta en compromiso de la seguridad de tarjetas. Estos incidentes no solo tienen impacto para las empresas en términos de reputación y costes o multas, sino también para el público en general, debido a que el robo de datos puede llevar a la suplantación de identidad.

La *tokenización* se define como:

*La sustitución de elementos o datos sensibles por un código equivalente no sensible. Lo anterior, llevado al ejemplo ilustrativo de las tarjetas de pago, consiste en la transformación del número PAN de la tarjeta<sup>21</sup> por un código sustitutivo vinculado a la misma y que no contiene datos sensibles.* (AEFI, 2020, p. 19)

De esa manera, se consigue un mayor nivel de seguridad en las transacciones, evitando riesgos de robo, fraudes o clonaciones.

En cuanto a las tarjetas físicas, este ha sido un ejemplo en el que se ha podido observar cómo las nuevas *FinTech* piensan distinto respecto a productos tradicionales. Para la banca tradicional, la emisión de tarjetas era masiva en función del producto que se contrataba, suponiendo altos costos de producción y entrega. Sin embargo, *challenger banks* como Revolut permiten a sus usuarios personalizar la tarjeta, escogiendo el color o diseño, mientras que los materiales de los que están hechas las tarjetas dependen del estatus dentro de la aplicación (*FinTech Finance*, 2019, pp- 1-2).

En el ámbito de emisión, otra de las innovaciones que ha surgido, principalmente en Asia, ha sido el sistema de pago QR, (Soon, 2008, pp. 59-78), que permite realizar pagos mediante el escaneo con el teléfono móvil de estos códigos, sin necesidad de incluir datos personales o números de cuenta.

Como se expuso anteriormente, parte de las *FinTech start-ups* y *TechFin* comienzan sus actividades en el entorno de emisión. Para ello, en los casos en los que no cuentan con la licencia y buscan una entrada rápida en el mercado, operan bajo modelos de BaaS, bajo acuerdos de colaboración o agencia con entidades financieras reguladas (AEFI, 2020, pp.

---

<sup>21</sup> *Personal account number*. Número personal de 16 dígitos que se encuentra en las tarjetas.

25-27). En este caso, se refiere a una innovación por parte de las entidades financieras (bancos) que identifican una nueva línea de negocio (servicio a las *FinTech* y *TechFin*), con la tecnología como habilitador (principalmente las conexiones e integraciones vía API).

### 3.2.2. *FinTech* adquirentes

La Asociación Española de *FinTech* e *InsurTech* describe las *FinTech* adquirentes como aquellas entidades proveedoras de servicios de pago que “se comprometen a aceptar, adquirir y procesar el pago por cuenta de un beneficiario, al que posteriormente liquidará los fondos” (AEFI, 2020, p. 33).

Estas actividades están principalmente enfocadas hacia los comercios, puesto que son los negocios quienes requieren de la provisión de servicios de recepción de pagos mediante tarjeta. Los servicios ofrecidos pueden agruparse a grandes rasgos en terminales de punto de venta (TPV) para el comercio físico, sistemas de adeudos domiciliarios para pagos recurrentes y soluciones de pasarelas de pago para el comercio electrónico.

Hasta el momento, el desarrollo del procesamiento de transacciones con tarjeta hasta ha sido ineficiente y costoso debido a las distintas partes que están involucradas en la compleja operativa (consumidor, banco emisor, las marcas UnionPay, Visa, Mastercard, entre otras, banco adquirente y comercio) (Sarin, 2020). Con la entrada en vigor de la PSD II, estos flujos se han simplificado, reduciendo partes involucradas y costos para los usuarios (ver Figura 7). En ese sentido, los costos asociados con las distintas partes que intervienen en la operación se reducen.

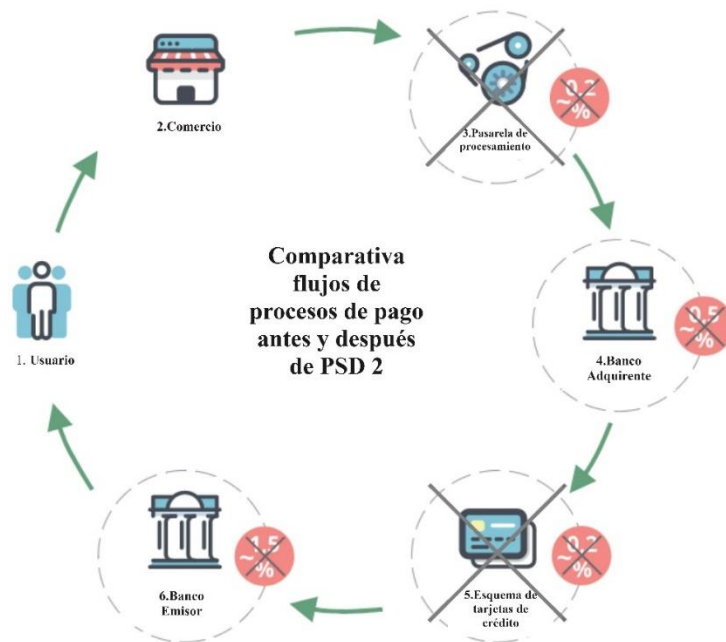


Figura 7. Comparativa de flujos en procesos de pagos antes y después de PSD II

Nota. Saltedge, 2021.

En este ámbito, uno de los progresos más relevantes ha sido la evolución del uso de los teléfonos u otro tipo de dispositivos como TPV, sin necesidad de emplear los aparatos específicos que tradicionalmente se venían utilizando (Accenture Research, 2020, p. 11).

Si bien el grueso de la actividad requiere de licencia debido a la captación de fondos del público (AEFI, 2020, pp. 24-63), existen servicios complementarios de optimización que están siendo cubiertos por *FinTechs*, como financiación, seguridad, gestión de devoluciones, facturación o automatización de servicios contables (AEFI, 2020, pp. 24-63).

### 3.2.3 Otras *FinTech* de pagos

Bajo este epígrafe se incluyen otros actores, como pueden ser los iniciadores de pagos, agregadores, las *SuperApps* o los proveedores de servicios a través de los modelos de finanzas integradas.

#### a) Iniciadores de pagos

Los iniciadores de pagos son una de las figuras reguladas bajo la Segunda Directiva de Pagos. La principal ventaja que ofrecen a los usuarios es realizar pagos sin necesidad de uso de tarjeta (Banco de España, 2020, pp.1-2). Su función principal es la de facilitar

el procesamiento de pagos entre consumidores y comercios a través de sistemas directos de pasarelas de pagos (Westlaw, 2020, pp.1-2).

El servicio de iniciación de pago se define como un “servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago” (art. 3.39 del RDL 19/2018). Los flujos operativos de los iniciadores de pagos pueden observarse en la Figura 8 . El proceso se inicia cuando el usuario desea comprar un producto en un comercio y decide pagar usando un iniciador de pagos (PISP). El PISP accede a la cuenta del usuario e inicia el pago en el comercio. El PSP del usuario ejecuta la transacción y el PISP notifica al comercio que la operación se ha iniciado. De esa manera, se cierra la operativa y el comercio entrega la mercancía.

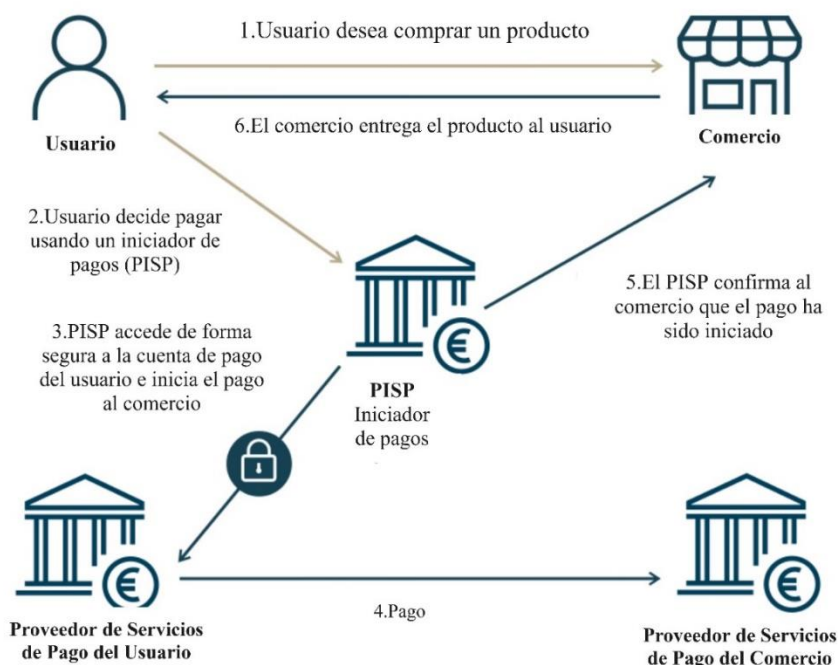


Figura 8. Flujo operativo de iniciadores de pagos bajo PSD II

Nota. Banco de Portugal, 2021

## b) Agregadores

Los servicios de agregación de pagos se definen en el artículo 3.18 del Real Decreto Ley 19/2018 como un “servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago”. En el ámbito español, este tipo de entidades requieren de registro ante el Banco de España (art. 3 del RD 736/2019).

Los flujos operativos de los agregadores de pagos pueden observarse en la Figura 9. La operativa se inicia con la autorización del usuario al proveedor de servicios de agregación de información de cuentas (agregador) para que acceda a las cuentas que el usuario tenga en distintas entidades financieras. De esa manera, el agregador accede de forma segura a los detalles de las distintas cuentas y las muestra en una única aplicación de forma consolidada.

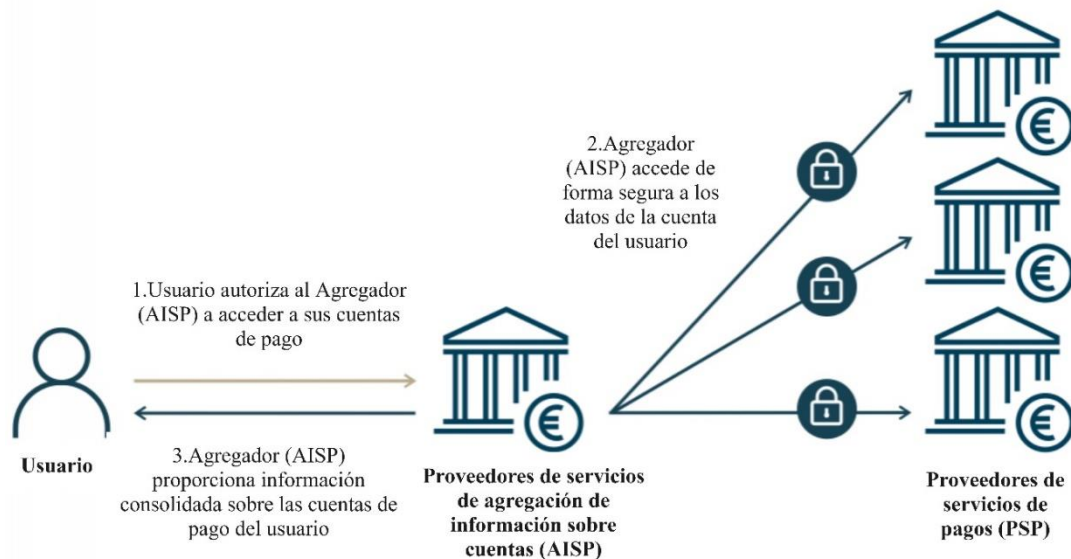


Figura 9. Flujo operativo de agregadores de pagos bajo PSD II

Nota. Banco de Portugal, 2021

Los proveedores de servicios de agregación de información cuentan con un potencial de crecimiento aún no explotado debido a las limitaciones propias de la regulación. Ello se debe a que la PSD II permite que estos terceros accedan únicamente a cuentas de pago, quedando fuera del ámbito de aplicación agregaciones de otro tipo de productos financieros como seguros, planes de pensiones o inversión. Como consecuencia de ello, los usuarios no llegan a obtener una visión integral de su situación financiera, por lo que los objetivos de análisis de los datos y su posible optimización de las finanzas no se llega a alcanzar por completo en la actualidad.

### c) Las SuperApp: *marketplace banking*

En 2010, Mike Lazaridis definió las SuperApp como una suerte de bazar o plataforma que ofrecía distintos servicios mediante combinaciones de tecnología

propia y de terceros (Larrauri, 2022, p.1). Los casos más conocidos son WeChat<sup>22</sup> y Alipay (Infopulse, 2019, pp.1-7). Estos nuevos modelos se caracterizan por hacer una reagrupación de productos y servicios financieros y no financieros de una manera novedosa, debido a que es el propio usuario quien escoge los servicios que quiere incluir en la SuperApp.

En lo que respecta a WeChat, a las funciones propias del programa relacionado con las redes sociales (sistema de mensajería, llamada y videollamada, almacenamiento de fotos y videos con posibilidad de compartir con amigos, sistema de contacto de usuarios), se añaden servicios de pagos (billetera digital, pagos *contactless*, pagos por QR y transferencias inmediatas entre particulares) y una pléyade de microaplicaciones que el usuario puede escoger para poder disfrutar de una aplicación que contiene todo lo que necesita (servicios de taxi, entretenimiento, comidas a domicilio, ventas de productos de segunda mano, seguros, inversiones, telefonía, comercio *online*, y préstamos entre otros) (Infopulse, 2019, pp. 1-7).

En ese sentido, las SuperApp se asimilarían a unas carcasas que vienen con unos productos predeterminados y a los que se pueden añadir cuantos quieran, a gusto de los consumidores. En el caso concreto de WeChat, se estaría hablando de más de un millón de microaplicaciones o miniprogramas disponibles para el usuario (Infopulse, 2019, pp. 1-7). Desde la perspectiva supervisora, estos modelos híbridos que contienen elementos regulados y no regulados presentan numerosos retos, dado que, desde el punto de transparencia, puede resultar confuso saber qué servicios están supervisados o garantizados y cuáles no. Tampoco resulta fácil identificar el cerco de actividades (miniprogramas) que caerían bajo la supervisión de las autoridades, cómo controlar las microaplicaciones de terceros relacionadas con servicios financieros o qué impacto podrían tener otros servicios no financieros sobre las partes reguladas.

Este tipo de modelos integrados o de todo en uno no es factible en la actualidad debido a que Europa está principalmente enfocada en modelos de pagos abiertos mediante API, pero no contemplan compartir datos con entidades terceras relativos a otro tipo de productos financieros (seguros, préstamos o inversión), ni mucho menos plantea el

---

<sup>22</sup> WeChat es una aplicación China creada en 2012, la cual agrupa funcionalidades propias de una aplicación social y de comunicación (mensajería, compartir fotos, videollamadas, llamadas telefónicas) con funcionalidades propias de pagos y microaplicaciones de terceros no financieras (por ejemplo, juegos) (Crunchbase, 2022).

mostrar modelos integrados en los que parte de los productos entren dentro del perímetro supervisor (financieros) y otros no (por ejemplo, oferta de viajes).

#### **d) Las finanzas integradas y su diferencia con los *Marketplace***

Las finanzas integradas (*embedded finance*) son una innovación enfocada en la eliminación de fricciones y mejora de la experiencia de los usuarios. Por este motivo, en muchas ocasiones se confunde con el modelo de negocio de *Marketplace*.

Desde el punto de vista del usuario, en ambos modelos se ofrece una experiencia integral, donde los pagos dejan de ser un proceso complejo de validaciones y se vuelven prácticamente invisibles. Esto es lo que, por lo general, se ha identificado como *embedded finance* (McKee, 2020, pp. 1-6). Sin embargo, el punto de partida (finalidad) de la aplicación es el elemento que se ha de tener en cuenta a la hora de distinguir entre *Marketplace* y finanzas integradas. En el supuesto de finanzas integradas, el proceso del usuario no comienza en una aplicación financiera, sino en una aplicación de un entorno no financiero (por ejemplo, plataformas de contratación de servicios de transporte, entrega a domicilio o plataformas de compra de productos).

En las finanzas integradas, los pagos son un elemento accesorio, pero necesario para perfeccionar la contratación del servicio. Dado que se trata de un paso más en la contratación y que, por lo general, produce fricciones o caídas de usuarios, las entidades buscan reducir el roce tratando de hacer el proceso de pago invisible o poco perceptible. La PSD II y sus normas técnicas de desarrollo han ayudado a estos modelos de negocios al permitir que los pagos de este tipo se sujeten a exenciones a la regla de autenticación reforzada de clientes (SCA) (art. 11 a 17 del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017).

A diferencia del *Marketplace*, donde pueden existir diversos proveedores financieros que dan soporte a la aplicación (la aplicación como frontal de diversos proveedores) (ver Figura 10), en *embedded finance* suele existir dos tipos de proveedores que brindan apoyo a la plataforma no financiera: (i) el proveedor de procesamiento y servicios de pagos, y (ii) proveedores de financiación y préstamo al consumo (específico de modelos de comercio en línea). Tanto los modelos de SuperApp como los de finanzas integradas cuentan con el mismo tipo de riesgos para los consumidores, principalmente centrados en la falta de transparencia sobre los entornos en los que están operando, quién es el proveedor real de los servicios, quién gestiona o procesa sus operaciones y, por tanto, quién es responsable en casos de fallos (por ejemplo, fraude o ataques de ciberseguridad).



Sumado a lo anterior, generalmente la operativa de ambos descansa sobre transacciones a través de tarjetas de crédito o débito, cuyos datos deben estar sujetos a niveles de seguridad especiales adoptados por la industria y denominados *Payment Card Industry (PCI) Data Security Standard* (Security Standards Council [PCI], 2018, pp. 1-39).

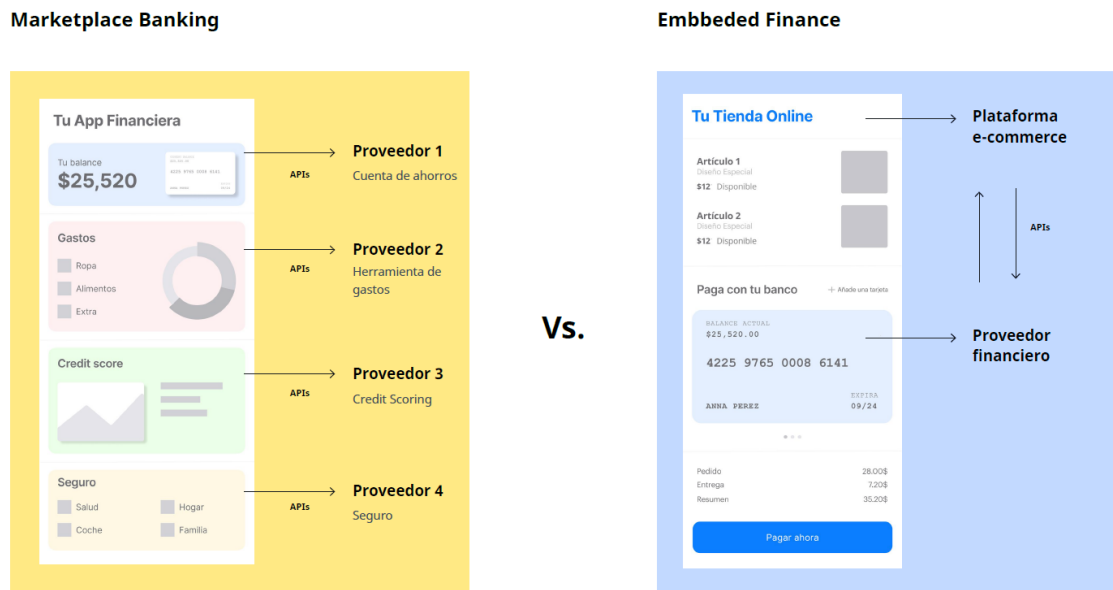


Figura 10. Comparativa Marketplace Banking con Embedded Finance

Nota. Tomado de *Economía colaborativa*, por Belvo, <https://belvo.com/es/productos/economia-colaborativa/>.

## 5. Recapitulación y observaciones sobre entidades intervinientes

El concepto de *PayTech* engloba una variedad de servicios que se encuentra en expansión. Asimismo, las *FinTech* que han entrado en esta actividad cuentan con morfologías distintas entre sí, lo que hace que su potencial y riesgos varíe de una a otra. Además, la aplicación de nuevas tecnologías, el enfoque en el cliente, el nuevo uso de datos y las estrategias de oferta de servicios hacen que estas entidades supongan una amenaza para la banca tradicional, por lo que deben plantear una estrategia de posicionamiento a futuro.

Debido a esto, los contextos normativos en torno a las *PayTech* deberán ser flexibles, basados en principios o actividades. De este modo, se logrará un entorno competitivo que pueda estar a la altura de otras regiones y una seguridad jurídica adecuada. Asimismo, se debería dejar la puerta abierta a nuevos tipos de modelos y participantes que puedan surgir

en los próximos años o que ya estén involucrados debido a las innovaciones existentes. Por ejemplo, en el ámbito de los criptoactivos, determinados tipos de *token* se tratarán como dinero electrónico y, por tanto, sujetos a la segunda directiva de pagos. Los proveedores de servicios futuros podrían no encajar en las categorizaciones existentes en la realidad o estas podrían resultar incompatibles u onerosas, requiriendo de distintos niveles o figuras aún por contemplar. Por esta razón, con el fin de diseñar normativas “a prueba de futuro”, será necesario establecer referencias a futuros modelos que puedan surgir, como una categoría general o por defecto.

Sin embargo, el impacto *FinTech* no solo tiene reflejo en los negocios de cara al público (ya sean personas naturales o legales), sino que también ha tenido un gran impacto en las infraestructuras de pagos mundiales, como se analiza a continuación.

## **6. *FinTech* 3.0 en infraestructuras**

### **6.1 *Planteamientos iniciales***

Una vez contempladas las novedades en contrapartes y frontales *FinTech* 3.0, se propuso realizar un estudio de las ineficiencias detectadas en las infraestructuras de pago globales, incluyendo las europeas o aquellas que afectan los pagos internacionales desde o hacia Europa. El motivo de llevar a cabo un análisis global se debe a que las infraestructuras de pago, hoy por hoy, son eminentemente internacionales y los mayores obstáculos no se identifican a nivel regional, sino cuando se evalúan operaciones más allá de la región europea.

Este tema está siendo discutido por los bancos centrales miembros del BIS, debido a que impiden el objetivo de inclusión financiera marcado por el G20 (OECD, 2018, pp. 6-28). Aplicando el método teleológico, se planean posibles acciones de política legislativa y administrativa que los bancos centrales e instituciones públicas están evaluando en la actualidad, y que tienen una base eminentemente tecnológica o *FinTech*.

Asimismo, se consideran los beneficios de una posible acción coordinada de carácter público-privado respecto las distintas problemáticas a las que se enfrentan las infraestructuras de pago internacionales en la actualidad. Para ello, se realiza un estudio principalmente enfocado en los informes emitidos al respecto por el BIS y las discusiones sostenidas en las conferencias de este órgano durante 2021 y 2022.

A lo largo de la sección, se pone de manifiesto que existe margen de mejora de estas problemáticas por medio del uso de innovaciones tecnológicas aplicadas al mundo de los pagos (*PayTech*) y a través de esquemas de colaboración público-privadas. Estas nuevas soluciones abren cuestiones jurídicas y de soberanía aún por dilucidar. Bajo dicho contexto, se aborda cuál es la foto actual en términos de gobernanza de los pagos internacionales y de los tipos de procesamientos que se dan en las estructuras de pagos internacionales, identificando los pagos minoristas como el sector de mayor margen de mejora y como el colectivo de mayor ineficiencia en términos de carga regulatoria versus materialidad de las transacciones.

Posteriormente, se afrontan los distintos tipos de problemáticas que se han identificado en los sistemas de pago internacionales que operan en la actualidad. A continuación, se desarrollan las distintas acciones de innovación tecnológico-financiera que los bancos centrales están evaluando en paralelo a nivel mundial, dentro del seno de la agenda del G20 y la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Este plan de acción ha sido coordinado principalmente por el FSB y el Comité de Pagos e Infraestructuras del BIS (CPMI). Finalmente, se enumeran acciones de tipo regulatorio y de gobernanza sobre las que se deberán tomar decisiones a lo largo de los próximos años.

## ***6.2 Acciones tomadas por los organismos internacionales***

Pese a que los sistemas de pagos internacionales tienen una estructura global, no existen marcos normativos de este tipo debido a que supondrían una cesión de soberanía de los países. Por lo contrario, se da una gran fragmentación regulatoria respecto a esta temática. A esto se suma el hecho de que los sistemas de pago en general se regulan mediante la conjunción de tres elementos (Benson, 2020, pp. 5-90): regulación nacional (de carácter público), esquemas de reglas de negocio y guías operativas (ambas de carácter privado).

La OCDE ha marcado como prioridades en su agenda la mejora de acceso a servicios financieros (inclusión financiera) y el “ofrecimiento de transacciones más convenientes, rápidas, seguras y oportunas” (OECD, 2018, p. 8). El documento subrayaba la necesidad de acatar acciones en términos de inclusión financiera mediante el uso de innovación de carácter tecnológico-financiera y la colaboración del sector público y privado. Como consecuencia de este mandato, en 2020, el FSB emitió un informe en el que acentuaba la

necesidad de implementar medidas que contribuyeran a la reducción de fricciones e ineficiencias en los sistemas de pagos (Financial Stability Board [FSB], 2020d, pp. 5-34).

Dentro de este esquema de prioridades, se establecía un plan de acción dividido en tres fases: (i) la evaluación de la situación (asignado al FSB), (ii) la construcción de bloques o *building blocks* (asignado al CPMI) y (iii) la hoja de ruta para la implantación de soluciones (FSB en coordinación con CPMI). Como parte del mandato asignado al CPMI, se desarrolló un informe denominado *Enhancing cross-border payments: building blocks of a global roadmap. Stage 2 report to the G20 – technical background report*, donde se identificaron los principales focos de mejora en las infraestructuras de pago internacionales (Committee on Payments and Markets Infrastructures [CPMI], 2020, pp. 1-11).

Finalmente, en octubre de 2020 salió a la luz el informe elaborado por el FSB en coordinación con el CPMI denominado *Enhancing Cross-border Payments. Stage 3 roadmap*, en el que se detalló un plan a cinco años (hasta 2025) involucrando a distintas autoridades a nivel mundial (Banco Mundial, IMF, FSB, CPMI, y FATF) (Financial Stability Board [FSB], 2020b, pp. 7-36).

### ***6.3 Panorama de los pagos internacionales en la actualidad***

En la apertura de la conferencia que el BIS ofreció el 18 de marzo de 2021 bajo el título *Pushing the frontiers of Payments*, Sir Jon Cunliffe indicó que hoy en día las transferencias internacionales pueden tardar hasta 10 días. Estas transferencias son las que cuentan con más fallos en el proceso y tienen un costo de hasta un 10 % del valor de la transacción (Bank of International Settlements [BIS], 2021a).

Por este motivo el sector de pagos minoristas se ha identificado como uno de los principales focos de ineficiencias. La razón de fondo es que los sistemas de pago se diseñaron inicialmente para realizar pagos corporativos, siendo posteriormente adaptados para minoristas. Sin embargo, hoy por hoy, las operaciones minoristas transfronterizas han adquirido un gran volumen debido a la globalización. Si se tiene en cuenta que cada vez hay más población inmigrante en los países, cuyo nivel adquisitivo es menor y la finalidad del pago es la recepción de fondos por sus familiares, generalmente en países emergentes, se llega a la conclusión de que es necesario buscar soluciones más eficientes y de menor costo, por lo que el sistema de infraestructuras de pago globales requiere de revisión.

Los gobiernos nacionales están trabajando en mejorar sus sistemas de pagos domésticos, pero los internacionales son más complejos debido a la cantidad de actores involucrados, así como los sistemas heredados o históricos tanto privados como públicos. Esto lleva a proponer la posibilidad de aceptar nuevas formas de infraestructura de pago que se desarrollen desde cero y nazcan libres de ineficiencias en los que los otros sistemas están trabajando, al tiempo que se trabaja en paralelo en la mejora de las infraestructuras de pago existentes. Dado que se trata de operativas y transfronterizas requieren de coordinación por parte de organismos globales como el propio BIS.

Esta apertura por parte de los bancos centrales se esboza incluso en el desarrollo de monedas digitales centrales que permitan mejoras en tiempos y costos a nivel internacional.

La necesidad de mejora de las estructuras existentes y desarrollo de nuevas estructuras más eficientes se aceleró especialmente durante el año 2020 debido a la pandemia, en la que se evidenció un aumento de volúmenes de compras y transferencias en línea, requiriendo de mejoras en las capacidades de procesamiento en los sistemas operativos de pagos a nivel mundial. El aumento del uso de la banca electrónica y del uso de teléfonos inteligentes, especialmente en el sector minorista, ha provocado un cambio en las expectativas del público en general, en términos de requisitos de experiencias de usuarios, tiempos de procesamiento y transparencia de las operativas.

#### ***6.4 Nociones previas: clasificaciones de los pagos***

El sistema de pagos se define como “el conjunto de instrumentos, procedimientos bancarios y, por lo general, sistemas interbancarios de transferencia de fondos que aseguran la circulación del dinero” (Banxico, 2021, p. 1). Los sistemas de pagos pueden tener carácter doméstico (centrados en un país o región) o internacional (enfocados en la gestión de pagos internacionales).

En función del valor de la transacción, se puede hablar de transacciones de alto valor (*wholesale*) y bajo valor (*retail*). Los sistemas de alto valor, mayoristas se diseñaron inicialmente para realizar liquidaciones entre sistemas de compensación, de mercados financieros y de intermediarios financieros. En la actualidad, se ha extendido a corporaciones que realizan operaciones por altas cantidades. En lo que respecta a España, este sistema es TARGET 2 – Banco de España (Banco de España, 2021, pp.1-2). Este sistema no compensa, sino que es una herramienta de liquidación bruta en tiempo real.

Esta característica es común y ampliamente adquirida por este tipo de sistemas a nivel global.

Los sistemas de bajo valor, minoristas hacen referencia a los canales empleados para la compensación y liquidación de transacciones de menor envergadura. Generalmente, estos sistemas operan con procesamientos en lote o de liquidación en diferido por considerarse no urgentes (Banxico, 2021, p.1). Asimismo, suelen englobar la liquidación de transferencias, adeudos, cheques, tarjetas y otro tipo de operaciones menores, como comisiones o tasas.

En el caso español, el Sistema Nacional de Compensación Electrónica (SNCE) es el sistema en vigor. La liquidación de sus transacciones se procesa a través de las cuentas de los participantes en TARGET 2 – Banco de España (Banco de España, 2021, p.1). Este canal es de uso generalizado para transacciones e interacciones entre consumidores (conocidas como P2P), empresas (conocidas como B2B) o empresas-consumidores (conocidas como B2C o C2B en función de la direccionalidad).

Como se argumentó anteriormente, estos pagos han heredado parte de la estructura y requerimientos de los pagos de alto valor, pese a que se manejen cantidades mucho menores. Esto provoca un desequilibrio entre los costos de procesamiento de este tipo de operativas (requerimientos regulatorios) frente a los ingresos que puedan traer a las instituciones. Debido a la falta de aplicación de un adecuado marco normativo de enfoque basado en riesgos para este tipo de pagos, los bancos se han centrado en los corredores de pagos de divisas que puedan traer mayor volumen de pagos minoristas (efecto agregador). Por otro lado, los pagos de bajo valor no gozaban de la opción de pagos en tiempo real. Esta tendencia ha ido cambiando a lo largo de los últimos años con desarrollos de iniciativas de pagos en tiempo real. Sin embargo, aún se encuentran limitadas a liquidaciones domésticas, principalmente en países desarrollados, lo que restringe los pagos instantáneos a nivel regional o internacional.

Por lo tanto, los pagos de bajo valor o minoristas parecen ser el principal foco de mejora en las infraestructuras de pago a nivel internacional. A este respecto, el FSB y el BIS han estado desarrollando distintos estudios sobre cuáles son los retos actuales a los que se enfrentan estos canales y cómo se pueden mejorar mediante el empleo de nuevas tecnologías con el fin de hacerlos más eficientes, reducir tiempos, costos y conseguir un mayor acceso y usabilidad por parte de poblaciones desatendidas.

## 6.5 Problemática de los sistemas de pagos

Actualmente, las infraestructuras de pagos globales se enfrentan a ciertos retos (Bank of International Settlements [BIS], 2020a, pp. 3-9), los cuales pueden agruparse dentro de los siguientes conceptos: (i) relacionados con el cumplimiento de normas (ya sea de fraude, blanqueo, sanciones o transparencia hacia consumidores y usuarios), (ii) relacionados con la propia operativa de pagos y (iii) de carácter tecnológico.

### 6.5.1 Cumplimiento normativo

Estos aspectos se centran en los requerimientos de identificación de clientes y su monitorización, que presentan retos desde el punto de vista de la protección de datos personales (transferencias de datos personales a terceros países) (Financial Stability Board [FSB], 2020b, pp. 3-6).

Respecto a los controles de prevención de blanqueo de capitales y financiación del terrorismo<sup>23</sup>, también existe la cuestión de los truncamientos de campos o la obligatoriedad de campos que han de contener los mensajes de pago. Estas ineficiencias derivan de que los sistemas de pagos son distintos por países o regiones, por lo que sus reglas técnicas difieren (por ejemplo, campos obligatorios por tipo de acción o límites de caracteres por cada línea y concepto). Esto hace que, cuando una transferencia internacional tenga que pasar por varios de estos sistemas, la información se corte o reagrupe, causando errores o pérdidas de información importantes para la monitorización de transacciones sospechosas o filtrados de sanciones internacionales. En caso de que los bancos cuenten con los controles adecuados, posiblemente pararán la operativa hasta que se obtenga la información requerida por la jurisdicción local, por lo que la transacción sufriría retrasos.

Estos eventos impactan en las ratios de procesamiento de operaciones automáticas (denominadas *Straight Through Processing*<sup>24</sup> o STP), provocando que su automatización se vea mermada en operativas transfronterizas debido a que requieren de procesos

---

<sup>23</sup> Existe la obligación de incorporar ciertos campos de información en las transacciones financieras con el fin de comprobar que las contrapartes, bancos intervinientes, jurisdicciones involucradas y conceptos no incumplen normativas relacionadas con el crimen financiero. A este requerimiento se le denomina “*travel rule*” y se aborda en detalle más adelante.

<sup>24</sup> El STP se define como “el procesamiento automatizado de un extremo a otro de las transacciones y / o transferencias de pago, incluida la finalización automática de la confirmación, comparación, generación, compensación y liquidación de instrucciones, sin la necesidad de volver a introducir o reformatear los datos” (Bank of International Settlements [BIS], 2021c, p. 1).

manuales de remediación. Los tiempos se alargan aún más si existen restricciones fiscales de moneda extranjera por parte de los países (por ejemplo, China (Cuatrecasas, 2011, pp. 1-3) y Argentina (Wainer, 2015, pp. 33-54)).

Existe otro foco de preocupación también relacionado con el cumplimiento normativo: la falta de transparencia hacia los consumidores y usuarios. Dado que existe un costo de gestión de las instituciones financieras (captura de datos, verificación de estos, controles de fraude, blanqueo de capitales y sanciones financieras internacionales, así como costos de corresponsalía), las comisiones repercutidas en los usuarios son en ocasiones altas y no transparentes (especialmente si se habla de divisas menos habituales). En conclusión, la complejidad y fragmentación regulatoria está impactando en las infraestructuras de pagos globales.

### 6.5.2 Operativo

Una transferencia internacional no solo requiere del banco del ordenante<sup>25</sup> y del banco del beneficiario<sup>26</sup>, sino que también suele haber numerosos bancos intermediarios (corresponsales<sup>27</sup>) involucrados en la cadena de pago que cobran comisiones (ver Figura 11).

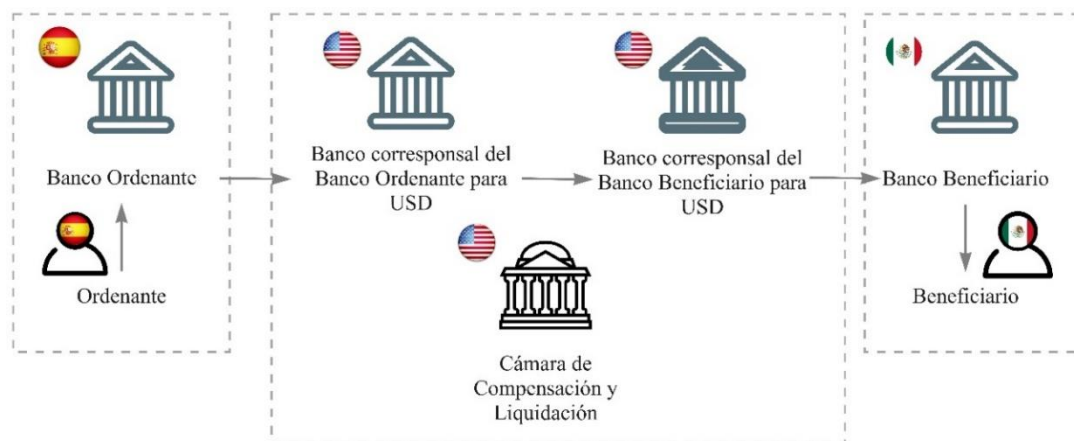


Figura 11. *Ejemplo de relaciones de corresponsalía para una operación en dólares entre un ordenante en España y un beneficiario en México*

Nota. Basado en Wandhöfer y Casu, 2018.

<sup>25</sup> El banco ordenante es el banco de la parte que emite una orden de pago o acuerda transferir fondos al beneficiario (European Central Bank, 2021a).

<sup>26</sup> El banco beneficiario es el banco del receptor de los fondos (European Central Bank, 2021a).

<sup>27</sup> La relación de corresponsalía se basa en un “acuerdo por el cual un banco (el banco de liquidación o prestación de servicios) realiza o recibe pagos (potencialmente realizando otros servicios bancarios) en nombre de otro banco (el cliente o banco de usuarios)” (European Central Bank, 2021a).



A modo de ejemplo, una transacción internacional empleando el canal de SWIFT requiere que los bancos involucrados tengan claves SWIFT intercambiadas<sup>28</sup> entre ellos para poder realizar transacciones. Sin embargo, debido a la carga de requerimientos de prevención de blanqueo y su costo, los bancos tienden a tener claves SWIFT abiertas únicamente con los bancos con los que realmente operan.

Esto lleva a que las probabilidades de que las claves intercambiadas con bancos de países emergentes sean bajas. Como resultado de ello, ordenar un pago a estos países suele requerir de numerosos bancos corresponsales hasta completar la cadena país-país (es decir, debido a que no hay relación directa, se tiene que diseñar una cadena de relaciones indirectas hasta llegar al banco del beneficiario). Este mecanismo se hace más complejo si se tiene en cuenta que no todos los bancos son participantes directos del sistema central de compensación y liquidación del país. En el escenario de que los usuarios operen con bancos miembros indirectos, se añadiría una capa más en el procesamiento de la operación. Por ese motivo, los pagos a países emergentes suelen requerir de más comisiones debido a que el número de intermediarios aumenta y en menor medida dentro de la EU. Para más detalle, ver un ejemplo de flujo operativo en EU en la Figura 12.

---

<sup>28</sup> Las claves SWIFT, también conocidas como SWIFT Relationship Management Application Keys o SWIFT RMA Key, son una forma de autenticación entre bancos que establece qué bancos han sido reconocidos o aceptados por otros para enviar o recibir mensajes dentro de la red de SWIFT. Previo a reconocer a estas contrapartes, se requiere haber llevado a cabo una diligencia debida del banco o institución en cuestión. De este modo, los bancos determinan con qué entidades aceptan trabajar dentro de la red (SWIFT, 2016).

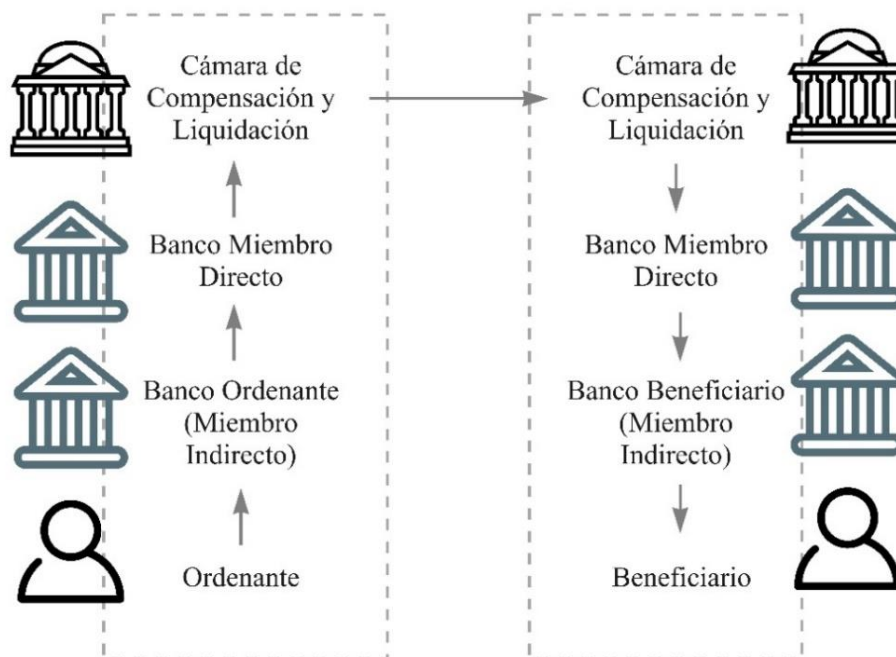


Figura 12. Modelo de transferencias entre dos países de zona SEPA con bancos miembros indirectos de las cámaras de compensación y liquidación

Nota. Elaboración propia.

En ese orden de ideas, los requerimientos regulatorios están provocando una exclusión de divisas menos relevantes, que, por lo general, son de países emergentes (Bank of International Settlements [BIS], 2021a).

Otra de las problemáticas operativas de los pagos internacionales se debe a las horas de corte u horas operacionales de las regiones (Bank of International Settlements [BIS], 2020a, pp. 1-11), lo que genera que ciertas operaciones se frenen cuando llegan a mercados que aún están cerrados y tengan que esperar a que los mercados abran. Un último punto de fricción es el hecho de que, para operar a nivel global, se requiere incurrir en costos de fondeo para acceder a los mercados internacionales (Bank of International Settlements [BIS], 2020a, pp. 1-11).

### 6.5.3 Tecnológico

Las infraestructuras de pago se apoyan en sistemas históricos (*legacy systems*) que se han desarrollado para realizar compensaciones y liquidaciones de posiciones de sus participantes mediante procesos en lote. Además, carecen de tecnología que permita a los supervisores el análisis de actividades en tiempo real o la analítica de grandes volúmenes de datos (Bank of International Settlements, 2020a, pp. 1-11). Este tipo de tecnologías,

aún en fase exploratoria, se engloban dentro del término *SupTech* y se analizan posteriormente.

Por otro lado, desde el punto de vista de experiencia de usuario, las estructuras de sistemas de pago empleadas en la actualidad se diseñaron inicialmente para los modelos de transacciones entre entidades (modelos B2B), que posteriormente se adaptaron a modelos *retail* (modelos B2C), haciendo que complejos los interfaces (Bank of International Settlements [BIS], 2021a). Estos problemas se traducen en barreras de acceso a pagos internacionales, pagos con altos costos, que llevan tiempo y no son transparentes (Bank of International Settlements [BIS], 2020a, pp. 1-11).

## **6.6 Innovación tecnológica como solución**

A la hora de plantearse cómo afrontar y resolver estos retos, el BIS y los bancos centrales han decidido no buscar una solución única, sino múltiples acciones en paralelo (Bank of International Settlements [BIS], 2021a). Esto se debe a que hoy en día muchas de las tecnologías en las que se basan las posibles propuestas aún se encuentran en testeo o desarrollo sin haberse podido evaluar por completo su potencial o sus riesgos.

Asimismo, debido a la necesidad de alta especialización técnica de ciertas medidas, las acciones que se están acatando han tomado un prisma de colaboración público-privada como se observa a continuación, distinguiendo entre soluciones de cumplimiento normativo, de mejora operativa, tecnológicas y de estrategia.

### **6.6.1 Cumplimiento normativo**

En general, los bancos centrales y la industria financiera han estado trabajando a lo largo de los últimos años en posibles soluciones sobre cómo gestionar operativas globales (pagos) frente a estructuras regulatorias fragmentadas (normas locales). En este sentido, se han desarrollado varias iniciativas en torno a las temáticas de identificación, verificación y armonización de los datos de pago.

### **a) Identificación y verificación**

La identificación y verificación de las personas o entidades que realizan las transacciones emanan de las obligaciones de prevención de blanqueo de capitales y financiación del terrorismo establecidas en las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) (Financial Action Task Force (FATF), 2012, pp. 10-131), y que han sido adoptados por sus miembros en las normativas locales. Sin embargo, el detalle de dicha adaptación ha creado diferencias de criterios y campos de datos requeridos por cada jurisdicción. Además, se debe tener en cuenta que estos datos identificativos pueden ser solicitados por bancos ordenantes o bancos beneficiarios, y que parte de esta información de carácter personal viaja a través de la cadena de pago, por lo que se realizan transferencias de datos internacionales.

A este respecto, han comenzado a surgir iniciativas gubernamentales de creación de identidades digitales de sus residentes. Suecia (BankID, 2021, p.21) ha sido un ejemplo temprano de modelo de colaboración público-privada en este sentido. En 2003, los principales bancos que operan en el país se asociaron para desarrollar una solución de identificación común para todos. Bank-ID es producto de esta colaboración y, en la actualidad, se concibe como una forma de identificación válida no solo por estos bancos, sino también por las autoridades y el sector privado en general.

La opción de desarrollo gubernamental sería más adecuada desde el punto de vista de seguridad y manejo de datos con los fines adecuados. Una iniciativa no gubernamental como la sueca podría suscitar dudas sobre el posible uso de datos con fines comerciales más allá del puro cumplimiento normativo. Cabría plantearse una solución semejante de identidad digital por jurisdicciones o regiones que posteriormente se validara a través de una entidad superior, siempre y cuando se base en unos estándares acordados entre los miembros, incluyendo la información requerida para las transacciones más comúnmente empleadas. Este es el enfoque que ha tomado la UE con su propuesta de identidad digital soberana dentro del marco de eIDAS 2, que será objeto de análisis crítico más adelante.

En ese sentido, se hablaría de un patrón similar al de la PSD II a la hora de verificar si hay saldo o no en una cuenta para proceder a un cargo. Dicho de otro modo, no se comparte el detalle del saldo en sí, sino que tan solo se confirma o rechaza. Aplicando una lógica similar, cualquier banco solicitaría a la entidad coordinadora confirmación de si las partes tienen identidad digital validada por alguno de los Estados Miembros. En caso de ser así, la operación se procesaría sin requerir ningún tipo de información

adicional. De este modo, se limitarían las transferencias de datos internacionales, al tiempo que se estaría validando identidad de las partes. Eso sí, la entidad coordinadora y sus miembros tendrían la responsabilidad de validar el cumplimiento de normativas de prevención de blanqueo de capitales y prevención de financiación del terrorismo.

#### **b) Armonización y calidad de los datos**

La armonización y calidad de los datos contenidos en la cadena de pagos no deja de ser un tema complejo. Si se toma SWIFT como ejemplo, se estaría frente a unos 300 tipos de mensajes agrupados en 10 grandes categorías (Oracle, 2021, pp.1-27). Cada mensaje tiene sus propias reglas y campos (obligatorios o voluntarios), por lo que homogeneizar los datos necesarios resulta ser una ardua tarea.

Si se tiene en cuenta que SWIFT es solo un canal para pagos internacionales<sup>29</sup> y que existen otras redes regionales (por ejemplo, SEPA en Europa) o domésticas (SPEI en México), con sus propios mensajes y reglas, la fragmentación se hace aún más evidente, lo que dificulta las tareas de monitorización de operativas sospechosas, fraudulentas o que puedan estar incumpliendo regímenes de sanciones financieras internacionales<sup>30</sup>. Ello provoca ineficiencias en los sistemas, así como la necesidad de operativas manuales de solicitud de información adicional, rechazos y reprocesamientos.

La necesidad de convergencia hacia estándares de intercambio de mensajes se ha hecho evidente. La ISO 20022<sup>31</sup> fue la solución anunciada por SWIFT en 2020 como modelo de convergencia ya previamente acordada por la comunidad bancaria en 2018. De esa manera, se espera un mayor nivel de estandarización y mejora de calidad de datos en las transacciones a nivel mundial. Debido a la envergadura del proyecto, contará con un periodo de solapamiento de los mensajes actuales con los nuevos entre el 2022 y el 2025 (SWIFT, 2021, p.1). Sin embargo, el propio CEO de SWIFT, Javier Pérez-Tasso,

---

<sup>29</sup> Según Javier Pérez-Tasso, CEO de SWIFT, actualmente existen más de 38 000 instituciones financieras a nivel mundial, de las cuales únicamente 11 000 están conectadas a la red SWIFT. Esto supone un 28,94 % aproximadamente del total instituciones (Bank of International Settlements [BIS], 2021a).

<sup>30</sup> A modo de ejemplo, en 2019, la zona euro contaba con varios sistemas de pago propios de la región, añadidos a los locales: EURO1/STEP1, STEP2 SCT Service, STEP2 SDD B2B Service, STEP2 SDD CORE Service y TARGET 2 (Bank of International Settlements [BIS], 2019b, p.1).

<sup>31</sup> ISO 20022 es un estándar de mensajes financieros y, en concreto, un estándar de mensajes de pagos e informes que utiliza una sintaxis estructurada conocida como Lenguaje de Mercado Extensible (“XML”); además de ser un diccionario de componentes de mensajes comunes que se puede reutilizar en otras transacciones financieras. Los estándares ISO 20022 abarcan el procesamiento de transacciones de valores y fondos, el financiamiento de operaciones bursátiles, el cambio de divisas e incluso los estándares de mensajes para los cajeros automáticos (ATM) y crean un lenguaje mundial común que permite a las contrapartes de los pagos comunicarse de manera eficaz, automatizada y cada vez más en tiempo real (J.P. Morgan, 2022, p.4).

advirtió que la ISO 20022 sirve como base de estandarización, pero se requerirán reglas adicionales de carácter local que pueden ser origen de nuevas divergencias de requerimientos y fragmentaciones (Bank of International Settlements [BIS], 2021a).

En el corto plazo, se están planteando soluciones que permitan detectar los criterios y reglas existentes en los países por los que la transacción viaje (esto es, país del banco originador, de los bancos corresponsales, de haberlos, y del banco beneficiario). Estas herramientas permitirían el filtrado inicial de los requerimientos de estas jurisdicciones y su validación inicial contra la información que el usuario ha incluido (prevalidación de interfaces), evitando que la operación se procese sin cumplir los requerimientos de todas las jurisdicciones (Bank of International Settlements [BIS], 2021a).

### **c) Uso de inteligencia artificial**

El uso de IA (*machine learning*) para la identificación de patrones de fraude y la reducción de falsos positivos en herramientas de blanqueo y sanciones es una acción principalmente promovida por las grandes estructuras privadas con el fin de disminuir los costos de procesamiento manual causados por ineficiencias en estos ámbitos. Las grandes compañías tecnológicas (*BigTech*) que en la actualidad están desarrollando sus propias estrategias de incursión en el mundo financiero, han estado aplicando estos modelos algorítmicos para la predicción del comportamiento de sus usuarios, e incluso herramientas propias de previsión de impagos de créditos (Frost et al., 2019, pp. 3-40).

Los bancos centrales son conscientes de que el sector privado lleva la delantera en este aspecto, por lo que se ha planteado tanto la posibilidad de compra de datos capturados por las entidades a través de fuentes no tradicionales como la adquisición de algoritmos y *know how* de las compañías, al existir alto nivel de demanda, pero poca oferta de expertos en la materia (Doerr et al., 2021, pp. 2-26).

Estos modelos de colaboración público-privada comenzaron a dar sus primeros pasos en determinadas jurisdicciones como consecuencia de la pandemia mundial. Un ejemplo de esta casuística ha sido el *Sveriges Riksbank* (banco central sueco), que procedió a la creación de una aplicación web abierta al mundo académico y a compañías privadas, donde no solo se podían extraer datos en tiempo real, sino que las propias empresas podían contribuir aportando datos no tradicionales (un restaurante podía reportar el número de reservas diarias). De este modo, existía un *crowdsourcing* de data en una forma colaborativa (Bank of International Settlements [BIS], 2021b).

Los usos de la IA por parte de los bancos centrales pueden agruparse en: (i) regulación y cumplimiento, (ii) estudios macroeconómicos y series temporales, (iii) datos de los mercados financieros, y (iv) componentes fundamentales o estructurales.

#### 6.6.2 Mejora operativa

Como se indicó anteriormente, existen problemas de tipo operativo relativos a la reducción de relaciones de corresponsalía para las divisas menores, lo que provoca un efecto de exclusión de estas, resultando en mayores costos y tiempos de procesamiento de cara al usuario final. Además, existen problemas de horas de corte operativo y fondeo.

Los pagos instantáneos están aflorando en numerosos países y regiones (en la actualidad existen unas 50 jurisdicciones invirtiendo en mejoras de sus infraestructuras de pago locales con foco en pagos en tiempo real) (Bank of International Settlements [BIS], 2021b). Sin embargo, el reto está en cómo hacer los pagos instantáneos entre jurisdicciones o regiones. Actualmente, en la UE, *TARGET Instant Payment Settlement* (TIP) permite la liquidación de pagos en tiempo real en euros (liquidación de operaciones de alto valor en la coyuntura de TARGET 2) (Banco de España, 2008, p. 1), y ha desarrollado la capacidad de abarcar más divisas. Como parte de este modelo experimental, ha alcanzado un acuerdo con el banco central sueco (*Sveriges Riksbank*) para liquidar en coronas suecas (Krona) (European Central Bank, 2020c, p. 1).

En paralelo, se está explorando el posible uso de la tecnología de registros distribuidos o DLT<sup>32</sup> como solución a esta problemática, puesto que permitiría el procesamiento casi inmediato de las transacciones prescindiendo de entidades corresponsales o agentes de liquidación (Bank of International Settlements [BIS], 2021b). De este modo, las entidades no tendrían que incurrir en costos de fraccionamiento de liquidez en las relaciones de procesamiento de operaciones de corresponsalía. Sin embargo, se debe tener en cuenta que la tecnología *Blockchain* no cumple con criterios de privacidad y secreto. A este respecto, se está trabajando en opciones de enmascaramiento de datos en las cadenas de *Blockchain* para evaluar la viabilidad de este tipo de actividades.

La aplicación de ISO 20022 a nivel global también permitiría reducir fraccionamientos en los procesamientos de operaciones, garantizando así una reducción de costos para el público en general (Bank of International Settlements [BIS], 2021b). Dado que las tareas

---

<sup>32</sup> Este concepto se analiza en detalle en secciones posteriores.

de corresponsalía y el procesamiento de transacciones son fuente de negocios de las instituciones financieras, es posible que en este aspecto existan intereses enfrentados.

En cuanto a otro de los elementos destacados desde el punto operativo (horas de corte y funcionamiento de mercados), tanto el FSB como el CPMI han propuesto una estrategia de alineamiento y extensión de las horas de operación (Financial Stability Board [FSB], 2020b, pp. 7-36). También se están buscando modelos de interoperabilidad entre sistemas de pago y acuerdos de cooperación entre regiones con el fin de automatizar los procesamientos de operaciones (Financial Stability Board [FSB], 2020b, pp. 7-36).

En lo que concierne a la cuestión de la falta de transparencia en cuanto al estado del procesamiento de la transacción y costos, en la actualidad se están planteando soluciones a través de API para poder hacer un seguimiento de la transacción y los costos asociados (Financial Stability Board [FSB], 2020b, pp. 7-36).

### 6.6.3 De carácter tecnológico

Las infraestructuras de pago actuales están basadas en una arquitectura de legados (*legacy systems*) que se ha ido acoplando o añadiendo a lo largo del tiempo sin considerar una revisión integral de esta. Además, los pagos de bajo valor sufren de ineficiencias producto de la falta de planeamiento específico para este tipo de operativas. En este sentido, la Deutsche Bundesbank ha presentado su propuesta al G20 denominada “*amplus*” (amplio) enfocada en los pagos minoristas, una proposición de desarrollos tecnológicos basada en tres pilares (Deutsche Bundesbank, 2021):

El primer pilar es el conocimiento de cliente (KYC) global. Se sugiere la creación de un identificador único de las contrapartes mantenido en bases centralizadas de las autoridades locales y supervisadas por el Fondo Monetario Internacional (FMI). Asimismo, se propone la aplicación de un enfoque basado en riesgos en los controles alrededor de las propias transacciones, traduciéndose en una menor carga de monitorización para pagos de bajo valor o procesados a través de corredores de pago seguros.

El segundo pilar es un esquema de asignación o direccionalidad (*addressability scheme*) que propone la introducción de un elemento identificador de las personas para poder asignarles las transacciones, independientemente de que tengan o no una cuenta bancaria abierta. Este elemento se combinaría con el teléfono de la persona y no con una



cuenta. Se estaría hablando de un concepto similar al número identificador de entidad jurídica (LEI, por sus siglas en inglés)<sup>33</sup> requerido para operaciones de corporaciones en mercados financieros, pero diseñado específicamente para personas y pequeñas empresas, dado que contará con mayor volumen y cobertura. Este identificador, combinado con la asignación de un número telefónico, permitiría el enrutamiento de la transacción, incluyendo potencialmente las operativas de proveedores de servicios financieros semirregulados o no regulados.

Finalmente, el último elemento es una infraestructura de pagos multilateral (IPSI). Bajo este concepto, el *Bundesbank* propone la creación de una única plataforma multilateral compartida para la liquidación de pagos transfronterizos cuyos participantes serían los propios bancos centrales. El operador de la plataforma sería el BIS, evitando horas de corte operativo. Bajo este esquema, los bancos centrales reemplazarían a los bancos corresponsales (el esquema sería banco ordenante, banco central del banco ordenante, banco central del banco beneficiario, banco beneficiario). Esta solución ofrece diversas ventajas en términos de tiempo, costos y transparencia de operaciones de bajo valor.

#### 6.6.4 Estratégicas: CBDC y gobernanza de las criptomonedas estables globales

En la actualidad, se está evaluando el uso de la tecnología DLT no solo como forma de creación de nuevas plataformas multilaterales de pagos internacionales, sino también para la emisión de monedas digitales, ya sea de origen público (bancos centrales) o privado (en cuyo caso, el BIS está contemplando en concreto las denominadas *stablecoins*) (Committee on Payments and Markets Infrastructures [CPMI], 2020, pp. 1-11).

Según Muñoz, A.F., estas monedas se definen como “una moneda digital emitida por un banco central y, por ello respaldada por este último mediante sus reservas” (V.V.A.A., 2021). Las CBDC o monedas digitales de bancos centrales han ganado interés en los últimos años, concibiéndose como una reacción a la aparición de criptomonedas (en concreto, global *stablecoins*) que podrían ser una amenaza para la estabilidad financiera de los países, así como su capacidad de impacto en las políticas monetarias de los bancos

---

<sup>33</sup> De acuerdo con el Ministerio de Justicia español, “El Identificador de Entidad Jurídica (LEI, por sus siglas en inglés) es un código global y único basado en el estándar ISO 17442, que se utiliza para identificar a las personas jurídicas que son parte en las transacciones financieras y para cumplir con los requisitos de información en los mercados financieros” (Ministerio de Justicia, 2021,p.1).

centrales (Committee on Payments and Markets Infrastructures [CPMI], 2018, pp. 7-31).

Actualmente, se encuentran en fase experimental, con puntos de discusión abiertos sobre temas relacionados con su naturaleza (moneda mayorista o para el público en general), el diseño (basado en cuentas abiertas en el propio banco central o *tokenizado*), el rol del banco central y la banca comercial, las características de privacidad de estas monedas versus los requerimientos de prevención de blanqueo de capitales y las posibles limitaciones (a modo de ejemplo, se está planteando que el euro digital se diseñe únicamente para el mercado europeo, las personas residentes en Europa y con un límite de cantidad) (Committee on Payments and Markets Infrastructures [CPMI], 2018, pp. 7-31).

Por otro lado, los bancos centrales son conscientes del creciente interés del público por las denominadas *stablecoins*, criptoactivos de emisión privada diseñados para solventar los riesgos de volatilidad de los que monedas como *bitcoin* adolecen. Las *stablecoins* se encuentran referenciadas o colateralizadas a valores reales, permitiendo que sus precios no fluctúen tanto como los del resto de criptomonedas (Mohanti, 2019, pp. 1-180). Pueden estar garantizadas por materias (en la actualidad hay casos referenciados a oro, diamantes o activos inmobiliarios), monedas o cestas de monedas, criptomonedas o basados en algoritmos (Anderson, 2019, pp. 5-60).

### ***6.7 Implicaciones regulatorias y de gobernanza de estas propuestas***

Estas acciones desarrolladas en paralelo conllevan un abundante número de implicaciones de tipo regulatorio y de gobernanza. A continuación, se enumeran las principales:

Primero, surge la necesidad de desarrollo de estructuras comunes o guías de alineamiento en términos regulatorios, de supervisión y monitorización (Financial Stability Board [FSB], 2020b, pp. 1-36). Este elemento irá en combinación con el desarrollo de modelos de mínimos estándares para los acuerdos multilaterales de niveles de servicio (Financial Stability Board [FSB], 2020b, pp. 1-36.).

La solución táctica (en el mundo privado) respecto a este requisito de alineamiento se traduce en la iniciativa de adopción masiva de los estándares ISO 20022 y acción coordinada de los estados y el sector privado a la hora de establecer reglas de desarrollo operativo y tecnológico.

Segundo, se requiere de la reevaluación de los requerimientos en torno a la prevención de blanqueo de capitales y prevención de financiación del terrorismo, incluyendo la necesidad de aplicar un enfoque basado en riesgos para pagos de bajo valor o corredores de pago considerados de bajo riesgo (por ejemplo, zona SEPA) (Bank of International Settlements [BIS], 2021a).

En relación con el punto anterior, existe la necesidad de homogeneización de requerimientos de información y campos, así como la conveniencia de un acuerdo entre autoridades encargadas de blanqueo y autoridades a cargo de asuntos de privacidad, especialmente en lo referente a la identidad digital. El desarrollo de guías o estándares comunes en todos los países reduciría el actual nivel de inseguridad respecto a este tema<sup>34</sup>.

Además, se podría proponer la modificación de marcos regulatorios respecto a las cámaras de compensación y liquidación, para permitir la entrada directa de otro tipo de participantes, reduciendo costos y tiempos de intermediación.

Tercero, se podría proponer el diseño de estructuras contractuales que permitan una mayor interoperabilidad, especialmente en campos como la promoción de pagos en tiempo real, plataformas de liquidación multdivisa o plataformas multilaterales de pagos internacionales (Financial Stability Board [FSB], 2020b, pp. 1-36).). Estas incluirían, entre otras, (i) posibles extensiones de los mandatos de los bancos centrales, (ii) acuerdos de participación de la divisa en el sistema o plataforma, (iii) acuerdos de conversión de la divisa en el sistema o plataforma y (iv) acuerdos marco de niveles de servicio entre los bancos centrales y la plataforma (Bank of International Settlements [BIS], 2021a).

Cuarto, en cuanto a las CBDC los bancos centrales deben evaluar si sus mandatos actuales han revisarse. Además, deberán evaluarse limitaciones regulatorias en términos de uso, público al que va dirigido y posible generación de intereses. No solo esto, sino que también sería conveniente tener en cuenta las implicaciones en la banca tradicional (reducción de depósitos, que desembocaría en un aumento de intereses en los préstamos a entidades y particulares.) Finalmente, se deberá observar cuáles son las implicaciones de las CBDC en la política monetaria (por ejemplo, la influencia y el tratamiento en los agregados monetarios para el cálculo y control de la inflación).

---

<sup>34</sup> Un ejemplo similar a este tipo de guías sería la emitida por el *European Data Protection Board* (EDPB) en diciembre de 2020 (European Data Protection Board, 2021, pp. 5-26).

Efectivamente, las criptomonedas estables podrían catalogarse de producto sustitutivo al dinero de curso legal, mermando la efectividad de la función de los bancos centrales como emisores únicos, y de sus políticas monetarias. Es por ello, que se hace relevante la necesidad de explorar el desarrollo de las CBDC para frenar este impacto.

Ha de considerarse que en lo concerniente a la gestión de la política monetaria (acciones de los bancos centrales para influir en la oferta monetaria, estabilidad de precios, tasas de interés y crecimiento económico), las criptomonedas estables podrían impactar la propia independencia de los bancos centrales y su capacidad de control sobre la oferta monetaria, ya que las criptomonedas (tal y como se ve en *FinTech 4.0*), se emiten fuera del control de las autoridades y tienen sus propias estrategias de políticas monetarias.

En el caso de que los bancos centrales adoptasen estrategias de CBDC basadas en tecnología de registros distribuidos se abrirían nuevas oportunidades, como por ejemplo la capacidad de bloqueo automático de flujos hacia contrapartes sancionadas, la programabilidad del dinero emitido o el ajuste de la oferta monetaria con mayor precisión.

Respecto a las global *stablecoins*, la incertidumbre radica en dos puntos: por un lado, en el diseño de un marco normativo híbrido (emisión privada con supervisión y controles públicos) y la reconceptualización del concepto del dinero o moneda, dado que se incluirían como monedas de aceptación generalizada las emitidas por entidades privadas. Por otro lado, el hecho de quién será la entidad encargada de la supervisión de estas *stablecoins* globales, puesto que si se opta por el criterio del país donde la entidad privada tiene su matriz, esto plantearía problemas de capacidad del regulador al controlar una moneda de carácter global, así como la extraterritorialidad de su capacidad de punición o supervisión.

Considerando lo anterior, parece que un modelo similar al que se aplica en la banca europea (supervisión local hasta que la entidad se vuelve relevante para el sistema financiero, accionando la supervisión directa bajo el BCE) podría extrapolarse a nivel mundial, en la figura de un “banco de bancos” que se encargaría de la supervisión de las criptomonedas estables globales. Esta solución, aunque lógica, conlleva el siempre dificultoso problema de una posible necesidad de cesión de soberanía por parte de los países.

Si bien parece que un modelo de cesión de competencias es complejo en términos de gobernanza, se puede comenzar con figuras más flexibles, como las de coordinador o guía de estándares mínimos, que podría recaer en el propio FMI o BIS. Sin embargo, estas figuras carecerían de un rol coercitivo, por lo que su capacidad de impacto se podría ver mermada.

### ***6.8 Recapitulación en lo afectante a infraestructuras de pago***

Se han identificado numerosos focos de ineficiencias en los sistemas de pago mundiales, especialmente en los pagos de menor valor, dificultando la inclusión financiera en países emergentes cuya divisa no es procesada como principal o de mayor volumen. Por su parte, el BIS reconoció ciertas brechas que, a lo largo de esta sección, se agruparon en problemáticas de cumplimiento, operativas y tecnológicas. Este organismo está centrando sus esfuerzos en varias innovaciones desde una perspectiva abierta, tanto en términos de uso de nuevas soluciones como en la apertura a colaboraciones con el sector privado.

A este respecto, en actualidad se está trabajando en varias iniciativas en paralelo, que incluyen no solo la modernización de las infraestructuras de pago existentes, sino también nuevas estructuras de pago futuras basadas en la DLT. Es por tal motivo que los marcos normativos relativos a mandatos de bancos centrales, derecho financiero y contractual deberán reevaluarse con base en las estrategias que finalmente se implanten.

Cabe concluir que resulta imposible converger en un único sistema de infraestructuras de pago globales o regulaciones homogéneas debido a las restricciones en términos de soberanía y cesión de competencias, por lo que la opción de coordinación por regiones parece ser la más factible (Bank of International Settlements [BIS], 2021a), siendo el propio BIS el “coordinador de coordinadores” en varios aspectos, tales como la validación de identidades digitales o los criterios de estándares operativos y tecnológicos a aplicar.

## **III. FINTECH 3.5: LAS FINANZAS ABIERTAS**

### **1. Introducción**

Bajo la denominación *FinTech 3.5* se engloba la manifestación y la expansión de la apertura de datos. Si *FinTech 3.0* aborda la apertura de datos y la consecuente desintermediación en pagos, *FinTech 3.5* plantea compartir datos financieros en general,

incluyendo productos de deuda, inversión o seguros. Por este motivo, se habla de interoperabilidad transversal de la industria financiera, puesto que los usuarios podrían concentrar potencialmente todos sus datos financieros en una sola aplicación, independientemente del tipo de producto.

Este fenómeno se da prácticamente en paralelo a la banca abierta de la UE; sin embargo, su foco son otras regiones como Asia o América Latina. Como señaló Muñoz, A.F., “*Open Finance* propone un intercambio de datos más profundo que llevará a compartir una gama más amplia de productos y servicios financieros. En la noción del *Open Finance* los consumidores comparten sus datos financieros con proveedores externos (TPP)” (Muñoz, 2021, p.3).

Las finanzas abiertas no son el final del cambio, sino que son un paso intermedio hacia una radicalización mayor al empoderamiento de los usuarios finales y el enfoque de colaboración. Es esta combinación en la que se enmarcan las finanzas abiertas como parte de la economía abierta (Charnley, 2021, pp. 1-4) (ver Figura 13)

La economía abierta va más allá del mundo de servicios financieros, incluyendo la posibilidad de que los usuarios puedan gestionar sus datos de forma transversal a cualquier industria. Asimismo, la experiencia financiera ya no se limita a entidades reguladas o incluso a *FinTechs*, sino que cualquier tipo de entidad podría llegar a tener ciertos roles financieros a través de los modelos de BaaS, *embedded finance* o equivalentes (ver ejemplo en la Figura 13).

## The Open Banking Evolution: From Beginning To Beyond

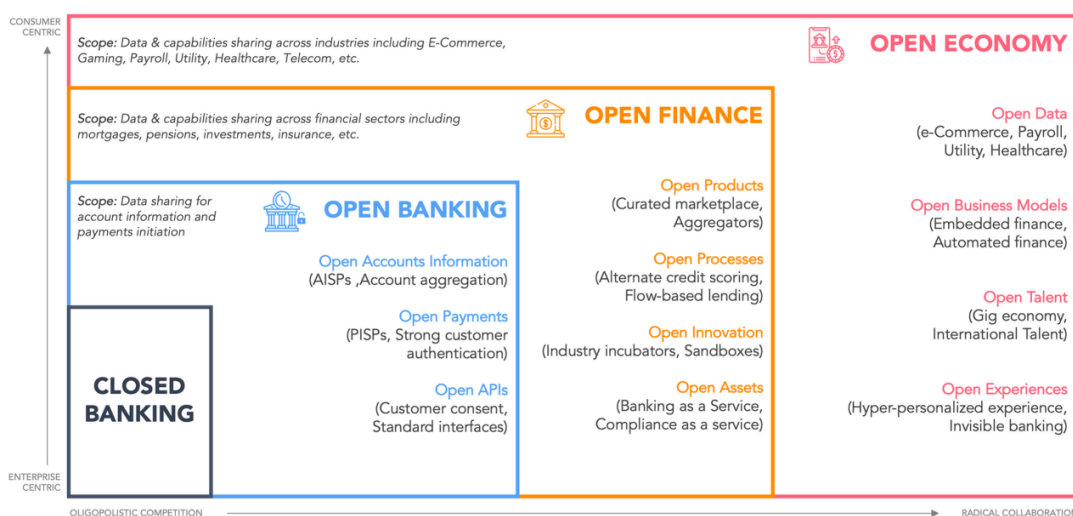


Figura 13. Evolución de la banca abierta: del inicio al más allá

Nota. Tomado de *From Open Banking to Open Data: Australia's Open Finance Journey Begins!*, por B. Charnley, <https://medium.com/open-finance-australia/from-open-banking-to-open-data-australias-open-finance-journey-begins-ce730f3270a7>

Dicho lo anterior, en esta sección se identifica el avance que se produce al pasar a hablar de banca abierta a finanzas abiertas. Seguidamente, se evalúan sus ventajas y riesgos, determinando los países emergentes como foco de esta tendencia. Si bien los sujetos obligados son los mismos que en *FinTech 3.0*, en *FinTech 3.5* las *BigTech* cobran importancia debido a su potencial impacto. Es por ello por lo que se abordan de manera específica dentro de esta sección.

Posteriormente, se exponen las nuevas actividades en *FinTech 3.5*, identificándolas por verticales propios de la banca tradicional (pasivo, activo, inversión y otros), así como por servicios con impacto horizontal o transversal (los denominados “*as a Service*”). Finalmente, se plantea la duda de si realmente se puede hablar de una desintermediación en finanzas y se lleva a cabo una evaluación para saber si estas actividades contaron con marcos normativos y de supervisión en 2022.

### 1.1 De la banca abierta a las finanzas abiertas

La *Financial Conduct Authority* de Reino Unido (UK FCA) indica que las finanzas abiertas “se basan en el principio de que los datos suministrados por y creados en nombre

de los clientes de servicios financieros son propiedad y están controlado por aquellos clientes” (Financial Conduct Authority, 2021b, p. 13).

Las finanzas abiertas son, una vez más, prueba de la aceleración que la innovación financiera estaba tomando con respecto a los plazos y tiempos regulatorios. Mediante la generación de marcos regulatorios amplios, los reguladores no europeos han tratado de crear las reglas del juego de los agentes *FinTech* que intervienen no solo en los servicios de pagos, sino también en otros verticales de la industria, como puedan ser inversión o seguros. Sin embargo, en la zona europea, la seguridad jurídica se centra en estos momentos en los verticales de pagos bajo la PSD II, dejando en situación de inseguridad jurídica otras actividades que han ido surgiendo a lo largo de estos años.

No solo eso, sino que, bajo la premisa de las finanzas abiertas, otras jurisdicciones (por lo general pertenecientes a países emergentes) empleaban este concepto para la preparación de marcos regulatorios más comprensivos, relegando la banca abierta de la PSD II a un subconjunto de requerimientos dentro de algo más grande: las finanzas abiertas (MENA *FinTech* Association, 2021, pp. 5-17). La Tabla 3 muestra con claridad cómo los modelos de finanzas abiertas permiten la apertura de datos en préstamos e hipotecas, ahorros e inversión, y seguros y pensiones. La formulación para cada uno de ellos no solo incluye visualización de los productos contratados, sino también la comparación, contratación y operativa general.

<b>Concepto</b>	<b>Acciones</b>	<b><i>Open Banking</i></b>	<b><i>Open Finance</i></b>
Cuentas y pagos	Visualización	Sí	Sí
	Comparación	Sí	Sí
	Iniciación	Sí	Sí
	Procesamiento/ bloqueo/ cancelación	Sí	Sí
Préstamos e hipotecas	Visualización	No	Sí
	Comparación	No	Sí
	Iniciación	No	Sí
	Procesamiento/ gestión/ cancelación	No	Sí
Ahorros e inversión	Visualización	No	Sí
	Comparación	No	Sí
	Iniciación	No	Sí
	Procesamiento/ gestión/ cancelación	No	Sí
Seguros y pensiones	Visualización	No	Sí
	Comparación	No	Sí
	Iniciación	No	Sí
	Procesamiento/ gestión/ cancelación	No	Sí

Tabla 3. *Análisis comparativo de servicios en banca y finanzas abiertas*

Nota. Elaboración propia.



Al igual que en la banca abierta, la herramienta de liberalización son los API; sin embargo, comienzan a identificarse modelos de innovación basados en la DLT. En esta etapa 3.5, el uso de estas tecnologías no se concibe como de absoluta descentralización, sino que sigue modelos de descentralización centralizada, dado que la DLT se emplea como una herramienta por parte de entidades legales centralizadas y las soluciones financieras *Blockchain* funcionan de forma centralizada, denominándose *permissioned Blockchains* (Muñoz, 2021)

Si bien la PSD II permitía el uso de estas innovaciones entre la banca y terceros en términos de pagos, su potencial es aún mayor. Esta posibilidad se explota en otros subsectores a través de las iniciativas regulatorias de finanzas abiertas que se están produciendo, principalmente en países en desarrollo. Por ello, la innovación aplicada a las finanzas en general ofrece ciertas ventajas y riesgos que se identifican a continuación. Asimismo, en el próximo apartado se evalúa por qué en este caso concreto el fenómeno no se está valorando desde la perspectiva europea, sino desde el lado de países emergentes.

## ***1.2 Ventajas para los usuarios: auto soberanía de datos y mejora de la gestión***

Las finanzas abiertas se están concibiendo como un progreso de la banca abierta en términos de datos, puesto que devuelven la hegemonía y el control de estos a sus usuarios, permitiendo, si lo desean, compartir datos financieros con terceros sin bloqueos. Si bien la PSD II abría datos de pagos, se pudo observar que existían limitaciones en la práctica (por ejemplo, no era posible visualizar y manejar datos de cuentas de inversión). Estas barreras se suprimen bajo el *open finance*.

Un ejemplo de su máxima expresión sería bajo un modelo de identidad digital soberana en el que la persona tiene una única identidad<sup>35</sup>, incluyendo su propio ecosistema financiero. De esa manera, los consumidores recuperarían la hegemonía sobre sus datos (a efectos prácticos, se vuelven originadores de los datos y encargados<sup>36</sup> de estos si se compara con la terminología aplicada en el Reglamento de protección de datos europeo).

---

<sup>35</sup> Las iniciativas europeas de revisión de la identidad digital y generación de una billetera de identidad digital se abordan específicamente en el capítulo de análisis crítico de iniciativas regulatorias.

<sup>36</sup> Artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o GDPR).

De este modo, el consumidor decide qué comparte, con quién comparte, cómo, cuándo y durante cuánto tiempo.

Si bien es cierto que uno de los principales puntos de beneficio es la devolución de los datos financieros a sus legítimos dueños, existe otro elemento trascendental del que no se ha investigado en profundidad hasta la fecha: el efecto de red que se genera por encima de cada uno de los verticales (pagos, préstamos, inversión y seguros), permitiendo una interoperabilidad transversal en la industria a través de plataformas y agregadores generalistas (no especializados simplemente en un producto como puedan ser los préstamos o las hipotecas) (MENA *FinTech* Association, 2021, pp. 5-17). Es decir, que el usuario operando en una plataforma de agrupación transversal (un agregador de todos los productos financieros del cliente en todas las entidades financieras que tenga) pueda identificar excesos de tesorería que tenga en la cuenta de la entidad “A” y pueda, desde la misma plataforma, asignar a un repago de deuda en “B” o a una inversión en el bono “C” de una forma ágil y sin fricciones.

Este tipo de plataformas permitirán, a su vez, soluciones de reducción de barreras de acceso a determinados servicios (por ejemplo, cantidades mínimas de inversión) o decremento de costos, intereses y comisiones (aumento de la transparencia del rango de oferta real y sus precios, mejorando la competencia). En ese sentido, el usuario se beneficia de varias formas en el *open finance*: (i) capacidad de acceso a servicios, (ii) visión realmente completa de su situación financiera, (iv) capacidad real de gestión de todos sus datos financieros, (iv) aumento y adaptación de la oferta de servicios, (v) optimización de su dinero (mejor asesoramiento), y (vi) nuevos productos y servicios (MENA *FinTech* Association, 2021, pp. 5-17; Financial Conduct Authority, 2021b, pp. 1-36).

Los beneficios que estos modelos puedan traer a la industria financiera dependen en gran medida del tipo de infraestructura del mercado que aplique *open finance* (mercados con mayor concentración de bancaria dejan la oferta financiera en manos de unos pocos, por lo que una estructura de *open finance* tendría alto impacto).

### **1.3 Riesgos**

También existen elementos de riesgo o barreras operativas que deben contemplarse. En lo que a riesgos se refiere, de nuevo, se pueden distinguir riesgos de frontales (de cara al público) y riesgos de *back* (de infraestructura o dinámicas de mercado), tal y como se

muestra en los ejemplos de la Tabla 4. Asimismo, los riesgos de cara al público pueden catalogarse como aquellos relacionados con la desprotección de consumidores y la falta de transparencia, el uso inadecuado de los datos e incluso el riesgo de exclusión financiera. En este contexto, los riesgos de infraestructuras o dinámicas de mercado pueden subdividirse entre aquellos que impactan la libre competencia y los relativos a operaciones y supervisión.

<b>Riesgos de cara al público (<i>front-end</i>)</b>	
Desprotección de consumidores y transparencia	Las finanzas abiertas implican la capacidad de las <i>FinTech</i> no solo de acceder a datos, sino también de actuar/operar en nombre del cliente (riesgos de fraude, riesgos operacionales, riesgos de ciberseguridad).
	Excesiva simplificación del producto con fines de comparación.
	Comparación basada en precios, costos e intereses, sin mostrar los riesgos (volatilidad, pérdida, coberturas).
Uso inadecuado de datos	Uso de datos con un propósito diferente al que el usuario cree que ha consentido, debido a la complejidad de términos, vaguedad de estos (autorización a compartir con terceros) o poca sofisticación del usuario.
	Uso de datos desactualizados, parciales o de calidad dudosa para la toma de decisiones o los algoritmos de cálculo ( <i>data points</i> ).
	Empleo de algoritmos discriminatorios.
Riesgos de exclusión	La negación de ciertos servicios a ciertas personas o colectivos en un vertical podrían extenderse a los demás debido a la transmisión de información entre sectores.
	Categorización de riesgo alto en un determinado servicio a ciertas personas o colectivos podría derivar en el encarecimiento de otros productos financieros debido a la transmisión de información entre sectores.
<b>Riesgos de infraestructura o dinámica de mercado (<i>back-end</i>)</b>	
Libre competencia	La entrada de las <i>BigTech</i> (mayor número y calidad de datos) podría crear un desequilibrio y concentración de la oferta (mudando de banca tradicional a las grandes tecnológicas).
	Los requerimientos regulatorios pueden conllevar la salida de participantes más pequeños o la huida a modelos financieros por debajo del radar supervisor.
Operaciones y supervisión	Aumento de contrapartes internas y complejidad de la operativa.
	Aumento de riesgos de ciberseguridad (más datos compartidos por más contrapartes).
	Falta de estandarización de las API.
	Falta de acuerdos de coordinación internacional.
	Aumento de la dependencia de terceros ( <i>outsourcing</i> y subcontrataciones).
	Entrada de terceros ( <i>FinTech</i> ) con menor conocimiento o concienciación de elementos de control en más verticales a la vez.

Tabla 4. *Visión general de los potenciales riesgos de las finanzas abiertas*

Nota. Elaboración propia.

#### **1.4 Protagonismo de los países emergentes en *FinTech* 3.5**

A diferencia de las iniciativas *FinTech* 3.0 adoptadas principalmente por los países desarrollados, las finanzas abiertas pueden concebirse como el salto cualitativo de los

países en vías de desarrollo a favor de los regímenes regulatorios de soporte a iniciativas *FinTech*. Es a partir de este momento donde se evidencia una separación entre *FinTech* 3.0 y *FinTech* 3.5, tanto desde el punto de vista público como privado.

En cuanto al aspecto público, surgen iniciativas regulatorias punteras fuera de la UE, que la propia región ha de tomar como ejemplo para considerar marcos normativos de 2022 en adelante (ver Tabla 5). Entre ellos, se puede identificar la implantación de modelos regulatorios de finanzas abiertas en Brasil, México, Australia, Hong Kong, India y Corea del Sur. Otros países han adoptado modelos de finanzas abiertas *de facto*, puesto que los supervisores los permiten sin penalizarse o considerarse ilegales. Tal es el caso de Singapur, Estados Unidos y China. Finalmente, tanto Bahrein como Chile cuentan con borradores de ley *FinTech*, que crearán perímetros legales de finanzas abiertas (ver Tabla 5. Iniciativas de banca y finanzas abiertas por país/región a diciembre de 2021).

A este respecto, la CE, dentro de su estrategia de finanzas digitales (Comisión Europea, 2020a, pp. 2-19) prevé que exista un marco normativo adecuado para 2024. No cabe sino observar que, desde 2020 (fecha de emisión del informe) hasta 2022, surgieron numerosas innovaciones y modelos de negocio que requieren de atención, por lo que cabe indicar que 2024 es una fecha demasiado lejana en contraste con la realidad de los mercados.

<b>País/ Región</b>	<b>Banca abierta</b>	<b>Finanzas abiertas</b>
Unión Europea	Sí	Inicio de estudio 2022
Reino Unido	Sí	Inicio de estudio 2022
Bahrain	Sí	En desarrollo
Japón	Sí	
Emiratos Árabes	Sí	
Turquía	Sí	
Suiza	<i>De facto</i> (industria)	
Nueva Zelanda	<i>De facto</i> (industria)	
Brasil		Sí
México		Sí
Australia		Sí
Hong Kong		Sí
India		Sí
Corea del Sur		Sí
Chile		En desarrollo
Singapur		<i>De facto</i> (industria)
Estados Unidos		<i>De facto</i> (industria)
China		<i>De facto</i> (industria)

Tabla 5. *Iniciativas de banca y finanzas abiertas por país/región a diciembre de 2021*

Nota. Elaboración propia.

De este modo, se puede comprobar cómo el interés general por *FinTech* proviene principalmente de países emergentes.

## 2. Los sujetos. Las *BigTech*

Si bien en esta etapa las instituciones financieras y las *FinTech* son agentes en activo, estos ya se analizaron previamente en la etapa *FinTech* 3.0. En la etapa 3.5 se realiza una evaluación de las *BigTech* en detalle debido a que tienen con la capacidad de presentar una amenaza real a la banca mediante la oferta de productos equivalente a la oferta bancaria total (cuentas, préstamos, inversión y seguros).

Además, las *BigTech* presentan un mayor reto regulatorio y de supervisión debido a que operan en otros mercados no financieros en la actualidad, e incluso las instituciones financieras dependen de las *BigTech* para la provisión de sus servicios a los clientes. En esta sección se analiza, por un lado, el fenómeno *BigTech*<sup>37</sup>.

### 2.1 El peso de los gigantes *BigTech* en las finanzas: el fenómeno *TechFin*

Las *BigTech* pueden definirse como “grandes conglomerados tecnológicos con extensas redes de clientes con negocios centrales en redes sociales, telecomunicaciones, búsqueda en Internet y comercio electrónico” (Adrian, 2021, pp. 1-5). Pese a que inicialmente se identifican estos grandes conglomerados con entidades operando a nivel mundial (por ejemplo, Amazon, Google, Facebook, Apple o Rakuten), en realidad existen *BigTechs* operando a nivel regional, como pueden ser los casos de Mercado Libre y Rappi (operando en América Latina), Jumia en Alemania o Grab en Singapur (Crisanto et al., 2022, pp. 1-35). Estas *BigTech* regionales suelen provenir de una segunda generación u oleada cuyo caso se analizará con mayor detenimiento.

Es característico de estas *BigTech* que, mediante estrategias de venta cruzada, consigan elevar el tráfico y la contratación de las distintas entidades del grupo, generando sinergias que se ven reflejadas en los ingresos. Estos modelos se han ido extendiendo hacia el mundo financiero a lo largo de los últimos años. En especial, se ha impulsado a razón de la crisis de la COVID-19. De esa manera, grandes conglomerados que parten del vertical tecnológico (*Tech*) han evolucionado hacia el adyacente financiero (motivo por el que se les denomina técnicamente *TechFin*).

---

<sup>37</sup> Su tratamiento regulatorio en UE se aborda más adelante

### 2.1.1 Operativa de las *BigTech* en finanzas

Las grandes tecnológicas han venido ofreciendo servicios digitales a grandes masas de clientes. Se apalancan en sus operativas para la captura de datos no solo entregados por los clientes, sino también generados por estos dentro de sus navegaciones por las webs y aplicaciones, dando a conocer preferencias (*likes*), intereses (grupos a los que se añaden), e incluso valor adquisitivo (volúmenes de compras y categorías de los productos comprados).

En un inicio, estas entidades podrían tender hacia una experimentación o fase exploratoria del mundo financiero a través de métodos más ligeros o no regulados, como podrían ser de (i) colaboración con entidades financieras reguladas, por los que se convertirían en agentes o referidores de estos; (ii) modelos de BaaS o *FinTech-as a Service* que se tratarán más adelante en detalle; (iii) distribuidores de productos financieros, en concreto préstamos o líneas de crédito ligados a la compra de los productos ofertados en sus plataformas; y (iv) alianzas estratégicas (Crisanto et al., 2022, pp. 1-35).

Los modelos de colaboración se limitan a la generación de flujos de potenciales clientes desde la aplicación de la *FinTech* hacia la institución financiera. De este modo, la *FinTech* se limita a referir al usuario hacia la entidad regulada, siendo esta quien presenta la documentación precontractual, realiza los controles de blanqueo de capitales y la totalidad de la operativa de la vida del cliente. Por lo tanto, la interacción con la *FinTech* es solo al inicio, como referencia hacia la entidad regulada.

En los modelos de BaaS o FaaS, el rol de la *FinTech* es mayor, debido a que, en ocasiones, hay ciertas delegaciones de la institución financiera hacia la propia *FinTech* (por ejemplo, pantallas de captura de información de cliente para la apertura o preevaluación de si este califica para el producto ofertado por la entidad financiera). En estos casos, la *FinTech* puede operar como un frontal tecnológico y canal de acceso habitual a los servicios financieros, y, por tanto, la relación con los clientes es habitual. Estos casos no quedan exentos de polémica en cuanto a la seguridad de los datos transmitidos durante la interacción entre las grandes tecnológicas y las instituciones financieras, así como qué tipo de control o diligencia debida debe llevar a cabo la institución financiera sobre la *BigTech* colaboradora. Un ejemplo de ello es la denuncia interpuesta en primera instancia ante el Juzgado de lo Mercantil Bilbao núm. 2, S 24-07-2015, n.º 197/2015, rec. 199/2015, n.º autos 199/2015 por parte de la Asociación de

Usuarios de Servicios Bancarios (AUSBANC) y la Asociación de Usuarios de Servicios Financieros (AUSBANC EMPRESAS). En dicha denuncia, BBVA había llegado a acuerdos de transferencias de archivos globales con Google y a la posibilidad de inicio de sesión vía el perfil de usuario de Facebook en Chile (Denuncia en Primera Instancia Juzgado de lo Mercantil Bilbao núm. 2, S 24-07-2015, nº 197/2015, rec. 199/2015, nº autos 199/2015 , 2015).

En los casos de distribución de productos financieros, se comienzan a ver escenarios en los que existe una obligación de la entidad financiera de declarar a la *BigTech* como proveedor de servicios o subcontratación críticos. Por este motivo, se incrementan los controles sobre la *BigTech* tal y como se abordará en el estudio del reglamento europeo de resiliencia operativa. Finalmente, en los casos de alianzas estratégicas, la *due diligence* a la que se someten las *BigTech* con el fin de catalogarse como aliados, deviene en un mayor nivel de control sobre la propia entidad y, dependiendo del tipo de alianza, la posible autorización por parte de supervisores.

Si bien la preferencia inicial es mantener estos modelos más livianos, a lo largo del tiempo se ha contemplado un incremento de la búsqueda de licencias propias con las que operan en los mercados financieros con el fin de crear nuevas líneas de negocio complementarias a las ya operadas, y de este modo, diversificar (Bethlendi y Szócs, 2022, p. 41; Zamil y Lawson, 2022, p. 1). Además, estos servicios financieros complementarios implican, a su vez, mejores retornos y contrataciones en los servicios que las plataformas ofertan como primarios, creando sinergias y mayor tráfico de operaciones. De esa manera, derivan a la postre en la potenciación de más puntos de datos relativos a los usuarios y sus comportamientos, ampliando su red (Staschen y Meagher, 202a, p. 2).

Dentro de estas estrategias de irrupción, también se han contemplado casos de adquisición de entidades *FinTech* operativas, que hayan demostrado tracción y cuya oferta de servicios o público objetivo encaje con las estrategias de las *BigTech* (Bethlendi y Szócs, 2022, p. 44). En general, las grandes empresas tecnológicas optan por modelos tanto de negocio-negocio (B2B) como de negocio-consumidor (B2C), incluyendo financiaciones a los comerciantes que operan dentro de sus plataformas, y sistemas de billeteras de pago y préstamos al consumo a los usuarios de la aplicación.

Por este motivo, se habla de finanzas de plataformas, refiriéndose a los servicios financieros que se integran dentro de la plataforma o la aplicación, generando comercios en línea y potenciando el crecimiento de usuarios, comerciantes y el tráfico a través de la

plataforma, extendiendo su actividad a sectores complementarios o adyacentes (Staschen y Meagher, 2022a, p.2).

Este potencial se hace aún más evidente en regiones con infraestructuras de pago inmaduras o en desarrollo. Por ejemplo, en América Latina, los servicios financieros ofertados a través de plataformas digitales y *FinTech* creció un promedio anual de un 147 % en el periodo entre 2013 y 2018 (Staschen y Meagher, 2022a, p. 2).

### 2.1.2 Evolución de las *TechFin* de empresas tecnológicas a empresas financieras

Las *TechFin* pueden adoptar diversos modelos de negocios con respecto a la banca tradicional, pudiendo optar por tener varios patrones de relación con la banca tradicional y otras *FinTech* (Tanda y Schena, 2019). Por lo general, son patrones evolutivos que se consolidan y que se mueven de una colaboración hacia una competencia, manteniéndose a menudo ambos aspectos en las fases finales, por lo que se podría hablar de una “co-competición” (por ejemplo, Amazon es a la vez colaborador tecnológico y competidor financiero de bancos).

En las fases iniciales o de exploración de entrada en el mundo financiero, estas entidades tenderán a funcionar como frontal tecnológico o generador de oportunidades de venta para entidades financieras, mejorando principalmente la experiencia de usuario para el consumidor final y los canales de distribución para la entidad financiera.

Un modelo operativo inicial derivado del anterior es el de actuar como proveedor tecnológico para las instituciones financieras tradicionales, cobrando por consumo de API o consumo de elementos de los sistemas bancarios desarrollados por las *TechFin*. Un ejemplo de ello es Ant Financial Technology, que en 2018 anunció un mayor enfoque a la provisión de servicios tecnológicos para entidades del sector financiero, virando su estrategia hacia servicios menos regulados y de mayor margen de ingresos (Zhang y Ruwitch, 2021, pp. 1-5).

La venta de la información de las *TechFin* para el enriquecimiento de datos relacionados con los requerimientos de cumplimiento puede ser otra variedad de colaboración posterior, siempre y cuando se cuente con los consentimientos expresos de los usuarios. En estos casos, los principales beneficiados son los modelos *RegTech*: eKYC (conocimiento digital del cliente), modelos de valoración de riesgos crediticios o modelos predictivos.



Finalmente, en fases de solicitud de licencias propias por parte de las *TechFin*, su papel pasaría a ser el de competidores de las instituciones establecidas, similar al caso de las grandes empresas tecnológicas (EBA, 2019b, pp. 6-34). Se puede considerar que este perfil de nuevos entrantes implicará un aumento de competencia, reducción de ingresos y aumento de rotación de clientela para las instituciones financieras ya establecidas (EBA, 2019b). En esta última fase, absorben el negocio financiero y, a su vez, siguen siendo proveedores tecnológicos de los bancos.

### 2.1.3 Pros y contras de la involucración de las *BigTech* en finanzas

Las *BigTech* parten con ciertas ventajas competitivas que pueden jugar tanto en pro como en contra de la estabilidad financiera y la protección a los consumidores. Por un lado, las *BigTech* parten de una amplia red y nutrida base de clientes que conocen debido al tráfico de datos que generan en sus plataformas, que muy a menudo es mucho más amplio y frecuente que la interacción con una institución financiera (el tiempo que el público pasa en Instagram, Facebook o WhatsApp es mucho mayor que el que pasa en la banca electrónica de su institución financiera de referencia).

Efectivamente, tanto la infraestructura tecnológica como el uso de herramientas de analítica de datos y *machine learning* les permite un mayor conocimiento y predicción de los comportamientos de sus usuarios y colaboradores. Igualmente, el uso de servicios de computación en la nube elimina restricciones, permitiendo aún mayores economías de escala. Además, estas entidades parten de un acceso a financiación consolidado que, incluso, puede verse particularmente beneficiado tras la obtención de licencias, en su valor de mercado o por acceso a los beneficios de financiación propios de las instituciones del mercado financiero (por ejemplo, líneas de los bancos centrales prestamista de último recurso) (Zamil y Lawson, 2022, p. 3).

De este modo, estos beneficios soportan la idea de que la gran utilidad que las *BigTech* pueden suponer para el sector financiero se centra en la capacidad de apoyar la inclusión financiera de poblaciones sub-bancarizadas o no bancarizadas. Ello se debe a su presente efecto de red y a su capacidad de ofrecer servicios a precios competitivos, mejorando tanto el acceso como el uso de productos financieros (Staschen y Meagher, 2022b, pp. 1-5; Gorjón, 2022, p. 7). Sin embargo, las plataformas tecnológicas tienen eminentemente dos grandes riesgos que acarrearán ya de sus sectores de origen y que, a menudo, han sido foco de sanciones: (i) la cuestión de la defensa de la competencia, puesto que tienden a

generar monopolios y a abusar de su posición dominante, y (ii) la inadecuada gestión de datos, problemática relacionada con temas de privacidad.

#### **a) Cuestiones de competencia**

Petit aborda el asunto de los monopolios *BigTech* desde dos puntos de vista: el del neoestructuralismo americano (que tiene una corriente similar en Europa a través del ordoliberalismo alemán) y el del bienestar del consumidor (Petit, 2020, pp. 6-28).

El primer punto de vista (neoestructuralismo) parte del análisis de la situación del monopolio desde una perspectiva estructural (de un vertical, producto o servicio). Esta corriente defiende que estos monopolios no son amenazas únicamente económicas, sino también de cierto calado político, dado que atentan contra los principios de la democracia (un poder distribuido entre distintos miembros sin que uno cause un grave desequilibrio de autoridad) (Petit, 2020, pp. 6-28). Respecto al neoestructuralismo, este se basa principalmente en el tamaño de las entidades y consideran que, con base en este, una entidad puede llegar a concentrar tanto poder económico que podría llegar a influir o dominar al Estado (*Louis K. Liggett Co. v. Lee*, 288 U.S. 517, 53 S. Ct. 481, 77 L. Ed. 929, 85 A.L.R. 699 (U.S. Mar. 13, 1933), 1933).

Estas corrientes advierten de numerosos riesgos de las *BigTech*, como pueden ser (i) el hecho de que tienen una posición dominante estructural, potenciada por la capacidad de uso de los datos generados en uno de sus verticales en otros mercados adyacentes como el financiero (Kahn, 2017, pp. 785-786); (ii) los precios predatorios incentivados por estrategias comerciales agresivas de captación masiva de clientes, que se ven recompensados por la adquisición de una multitud de servicios una vez dentro de la plataforma; (iii) el apalancamiento ofensivo, mediante el crecimiento en el mercado financiero partiendo del mercado tecnológico y del apalancamiento defensivo, a través de la adquisición de potenciales competidores antes de que sean demasiado grandes; (iv) los filtros al ser intermediarios (*gatekeeping*), en los que se trasladan los costos y riesgos a los participantes, beneficiándose de las comisiones; y (v) los daños políticos, en el sentido de que algunas plataformas controlan los medios (por ejemplo, Google tiene capacidad de mostrar las noticias prioritarias o favorecer la compra de sus propios productos y servicios, *Google shopping*) (Commission Decision of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search

(Shopping)), 2017). Además, las plataformas gozan de un fuerte poder de *lobby* (Petit, 2020, pp. 6-28).

En ese sentido, el neoestructuralismo y el ordoliberalismo alemán proponen rebalancear estas situaciones mediante el fraccionamiento de estos conglomerados (similar al caso de Ant Financial en China), y a través de la prohibición de fusiones y adquisiciones que puedan conducir a situaciones de abuso de posición dominante o que pongan en peligro la libre competencia en los mercados (Petit, 2020, pp. 6-28).

Respecto al segundo punto de vista sobre cómo tratar los monopolios *BigTech*, esto es, la posición de bienestar del consumidor, cuya teoría se ha implementado cada vez más frecuentemente en la UE, parte de la concepción de que las plataformas adquieren posición de monopolio cuando en la práctica se convierten en el único proveedor de servicios válido, lo que puede generar barreras de acceso al mercado y abusos en el servicio. Estos casos suelen darse especialmente en aquellos mercados en los que la regulación no distingue entre este tipo de entidades y el resto de las participantes, lo que implica requerimientos regulatorios laxos para su capacidad de poder o sanciones consideradas de bajo daño para la plataforma debido a su valor insignificante o no material (Petit, 2020, pp. 6-28).

La corriente de la teoría del bienestar del consumidor busca mantener la competencia en los mercados por el bien de los consumidores o con el objetivo de mantener una adecuada eficiencia en estos (Judgment of the Court (Grand Chamber) of 6 September 2017. *Intel Corp. v European Commission*, 2017). De este modo, se considera que la situación de posición dominante y monopolio no solo se basa en el tamaño en el vertical, como establece el neoestructuralismo, sino que dota de nuevas herramientas o criterios a la hora de dilucidar la situación (Petit, 2020, pp. 6-28). Esta posición permite contemplar situaciones de monopolios incluso en casos de servicios gratuitos de cara a los usuarios, como los ofrecidos por Google. De esa manera, se interpreta (i) que existe una transferencia de valor a través de los datos compartidos o generados, que son monetizados y explotados por la plataforma; y (ii) que el monopolio de mercados se define por la ausencia de categorías de productos o servicios sustitutivos a los que el usuario pueda saltar en caso de cambios con impacto negativo para los usuarios en términos de precios o de calidad del servicio (Petit, 2020, pp. 6-28).

Siguiendo estos principios, y con el fin de hacer a las plataformas responsables de sus actividades, la UE desarrolló dos propuestas normativas con enfoque en la libre

competencia digital y el control de estas *BigTech*. En ese sentido, se desarrollaron el DMA<sup>38</sup> y el DSA<sup>39</sup>. Sin embargo, estos reglamentos son transversales (no específicas del sector financiero), por lo que pecan de demasiado genéricos para el propósito del control de las actividades de las *BigTech* en los mercados financieros tal. Esta posición se sustentará en la segunda parte de la tesis con el análisis crítico de ambos reglamentos.

### **b) La gestión de datos y el problema de la privacidad**

En cuanto al segundo gran riesgo (la inadecuada gestión de datos y la problemática de la privacidad), este es un asunto ya tratado y sancionado en numerosas ocasiones, que tiene su base, por lo general, en una excesiva captura de datos, su uso con fines distintos a los inicialmente recabados y la venta de estos a terceras partes sin el adecuado consentimiento del afectado.

Las *BigTech* cuentan con un cierto poder de control o soberanía sobre los datos de los usuarios de sus plataformas, puesto que es la única forma de acceder a sus servicios; es decir, existe cierta conciencia de resignación o aceptación de que la entrega de datos es el peaje que se tiene que pagar para gozar de los beneficios propios de la plataforma. Esta capacidad se extiende, dado que, por lo general, los avisos de privacidad de estos gigantes tecnológicos incluyen la autorización del usuario a compartir los datos con todas las entidades del grupo e incluso con terceros colaboradores (Crisanto et al., 2022, pp. 1-35).

Igualmente, la transferencia o portabilidad de datos es discrepante entre las entidades sujetas a la segunda directiva de servicios de pago, por la que se exige la apertura y transferencia de datos vía API, frente a los requerimientos bajo el Reglamento General de Protección de Datos (GDPR)<sup>40</sup>. Esto limita la obligación de que esta sea técnicamente posible. De esa manera, las grandes empresas tecnológicas podrán acceder a datos de la banca, pero el flujo inverso no será posible (Padilla, 2020, p. 15). En el ámbito competitivo, el GDPR parece haber tenido el efecto contrario al esperado: las *BigTech* han continuado avanzando en términos de beneficios y clientela, mientras que las

---

<sup>38</sup> Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

<sup>39</sup> Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

<sup>40</sup> Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)

entidades más pequeñas acusan los costos de cumplimiento (Frey y Presidente, 2022, pp. 1-5).

#### 2.1.4 La cuestión supervisora

Desde el punto de vista supervisor, hoy en día las *BigTech* plantean retos aún no resueltos. El primero de ellos se debe a las relaciones de interdependencia de varios tipos, ya sean internas o externas. Las interdependencias internas se dan entre entidades del mismo grupo, como, por ejemplo, dependencias de las divisiones que ofrecen servicios financieros (regulados), de las divisiones que ofrecen servicios tecnológicos (no regulados) o los negocios de comercio electrónico, o incluso tercerización intragrupo de operativa<sup>41</sup>.

Las interdependencias externas se dan entre las *BigTech*, entidades reguladas e incluso supervisores. Existen casos como los de los servicios de computación en la nube, en los que estos (por ejemplo, Microsoft) son proveedores de otros gigantes tecnológicos (por ejemplo, Mercado Libre). Los servicios ofertados, por tanto, pueden ser los propios de su actividad en la plataforma, servicios tecnológicos de infraestructura o incluso servicios financieros (Crisanto et al., 2022, pp. 1-35).

Como se observa en la Figura 14, conglomerados como Alibaba o Amazon actualmente ofrecen servicios no solo propios de su actividad de origen, denominados *core*, como el comercio electrónico o los servicios digitales, sino que han extendido su actividad a servicios de tecnología (servicios de nube o de analítica de datos) y financieros. Por otra parte, en la Figura 14 se muestran ejemplos de cómo las *BigTech* se han centrado principalmente en pagos y provisión de créditos como extensión natural a sus negocios principales, que cuentan con gran afluencia de pagos y compra a plazos o préstamos como servicios complementarios. Sin embargo, también se aprecian incursiones en aspectos relacionados con la gestión de activos, los seguros y el desarrollo de negocios que requieren licencia bancaria completa.

---

<sup>41</sup> Se refiere a la externalización de servicios a entidades del mismo grupo consolidado.

	Core services		Financial services					Technology services		
Big tech	E-commerce	Digital consumer services <sup>#</sup>	Banking <sup>%</sup>	Credit provision	Payments	Asset management	Insurance	Cloud-based solutions <sup>*</sup>	Data analytics	Other <sup>&amp;</sup>
<b>Alibaba (Ant Group)</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Amazon</b>	✓	✓		✓	✓		✓	✓	✓	✓
<b>Grab</b>		✓	✓	✓	✓	✓	✓		✓	
<b>Jumia</b>	✓	✓		✓	✓					
<b>Mercado Libre</b>	✓		✓	✓	✓	✓				
<b>Rakuten</b>	✓	✓	✓	✓	✓	✓	✓		✓	✓

Figura 14. *Ejemplo de oferta de servicios BigTech*

Nota. Tomado de *Big tech interdependencies – a key policy blind spot*, por J. Crisanto, 2022, Bank of International Settlements.

Esta extensión de servicios por parte de las *BigTech* provoca el aumento de interdependencias entre entidades no reguladas y reguladas, entre servicios financieros y no financieros, que suponen un auténtico desafío supervisor, dado que se extienden más allá de su perímetro de control, generando riesgos no monitorizados (Staschen y Meagher, 2022a, p. 2). Esto incluye potenciales riesgos de contagio con impacto en la estabilidad financiera, así como riesgos de continuidad de negocio.

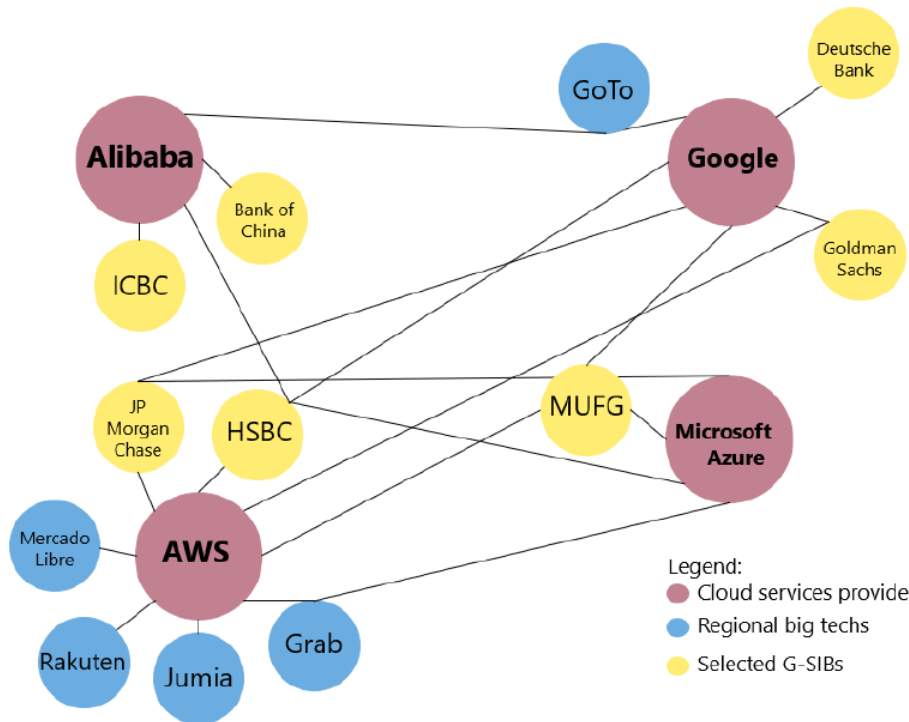


Figura 15. Ejemplo de dependencias y relaciones entre proveedores de servicios de computación en la nube, BigTech regionales y entidades financieras sistémicas

Nota. Tomado de *Big tech interdependencies – a key policy blind spot*, por J. Crisanto, 2022, Bank of International Settlements.

A modo de ejemplo, se muestra cómo los grandes bancos como HSBC o JP Morgan Chase dependen de los servicios en la nube proporcionados por Amazon a través de Amazon Web Services (AWS). Este grupo, a su vez, cuenta con una división que proporciona servicios financieros de todo tipo, por lo que se generan conflictos de interés en caso de una inadecuada gestión de los datos y un riesgo de no aislar adecuadamente la información. Del mismo modo, AWS es contratado por otras BigTech, como son Rakuten, Jumia, Grab o Mercado Libre. Estas, por su parte, cuentan con servicios principales que compiten con los del grupo Amazon, y con servicios financieros de los bancos y del propio Amazon. Este tipo de dependencias y relaciones conflictivas se repiten en otros servicios de nube, como Microsoft, Google o Alibaba.

La incertidumbre supervisora no se limita a su rol como proveedores de servicios tecnológicos, sino que se complica aún más con ocasión de la solicitud de licencias de tipo financiero. En esta coyuntura, por lo general, la regulación se enfoca en los riesgos que presentan estas entidades en el mundo financiero, pero no entran a elaborar en los riesgos inherentes a las propias plataformas por ser entidades sobre las que subyace el componente *tech* con sus correspondientes riesgos operacionales (Zamil & Lawson, 2022,

p. 2). En ese sentido, puede darse el supuesto de *uneven playing field* entre los grandes grupos financieros que cualifican como *Global Systemically Important Financial Institution* (GSIFI) o *Global Systemically Important Insurers* (G-SIIS) y las *BigTech* que entran en el mercado y acarrear en la práctica riesgos equivalentes o mayores a las anteriores. Estos casos se hacen patentes en los procesos de obtención de licencias por parte de estas entidades que, por lo general, se tratan como cualquier otro solicitante, sin identificar adecuadamente los requerimientos necesarios en el mundo financiero para su adecuado control.

En este contexto, cabe plantearse si la zona euro no requerirá a largo plazo de un supervisor *BigTech* con capacidad de evaluación del riesgo de una forma holística, permitiendo perímetros de control híbridos que supervisen el trasvase de riesgos entre las industrias en que la *BigTech* opere, soportado por los supervisores propios de cada industria. Si bien ya comienzan a contemplarse controles dirigidos al colectivo *BigTech* a través de la regulación en la región (principalmente DORA<sup>42</sup>, MiCA<sup>43</sup> –para el caso de que los gigantes tecnológicos sean emisores de cierto tipo de criptoactivos–, DMA y DSA), estas iniciativas parecen ser parciales y puede cuestionarse si su efecto no será similar al ya indicado con GDPR (bajo o nulo impacto en los beneficios y expansión del poder de las plataformas tecnológicas).

### **3. Las actividades. Análisis de la transformación *FinTech* 3.5 desde la perspectiva de sus productos y servicios**

Una vez identificados los actores existentes en la etapa *FinTech* 3.5, esto es, la acumulación de los vistos en la etapa 3.0, más los que cobran mayor protagonismo en las finanzas abiertas (*BigTech*), se procedió a delimitar las actividades propias de *FinTech* 3.5. En esta etapa, el proceso de desagregación continúa más allá de los propios pagos; sin embargo, se trata de una suerte de desagregación centralizada, puesto que los nuevos participantes son entidades identificadas (centralizadas) que, en ocasiones, llevan a cabo reagrupaciones de servicios financieros y no financieros de forma distinta a las entidades tradicionales.

Partiendo de la definición amplia del concepto *FinTech* empleada en esta tesis (desarrollo de innovaciones tecnológicas en entornos digitales con impacto material real

---

<sup>42</sup> Esta iniciativa se analiza en detalle más adelante.

<sup>43</sup> Esta iniciativa se analiza en detalle más adelante.



o potencial en la industria financiera y, por ende, en sus infraestructuras y participantes (consumidores, entidades, instituciones financieras y autoridades)), el ecosistema de las tecnofinanzas 3.5 engloba varias actividades de la industria financiera, como se muestra en la Figura 16. Por este motivo, es importante delinear e identificar estas actividades, que no solo se circunscriben a la esfera de la actividad del sector privado, sino también al sector público.

El primer paso es diferenciar aquellos avances que impactan en los actores privados frente a las innovaciones que impactan en la propia supervisión pública (las herramientas público-administrativas para la innovación del sector financiero o *SupTech*). En el sector privado y público de carácter tecnológico, las innovaciones se han identificado en su mayoría con el sufijo “Tech”. En ese sentido, esta sección aborda las innovaciones del sector privado en actividades verticales de pasivo (*PayTech*), activo (*CrediTech*, *Crowdfunding* y *Crowdlending*), inversión (*WealthTech*) y otros servicios financieros o auxiliares al mundo financiero (*InsurTech*).

Por otro lado, siguiendo la definición *FinTech* desarrollada en el presente trabajo, se analizan no solo innovaciones privadas, sino también las públicas o de supervisión, que a efectos de esta sección se identifican como *RegTech-SupTech*.

Finalmente, existen también desarrollos de actividades de innovación en el sector privado que podrían catalogarse como “horizontales” o “transversales”, puesto que afectan a todos sus verticales (pasivo, activo, inversión y otros) y han proliferado a lo largo de los últimos años, identificándose como servicios “as a Service”.

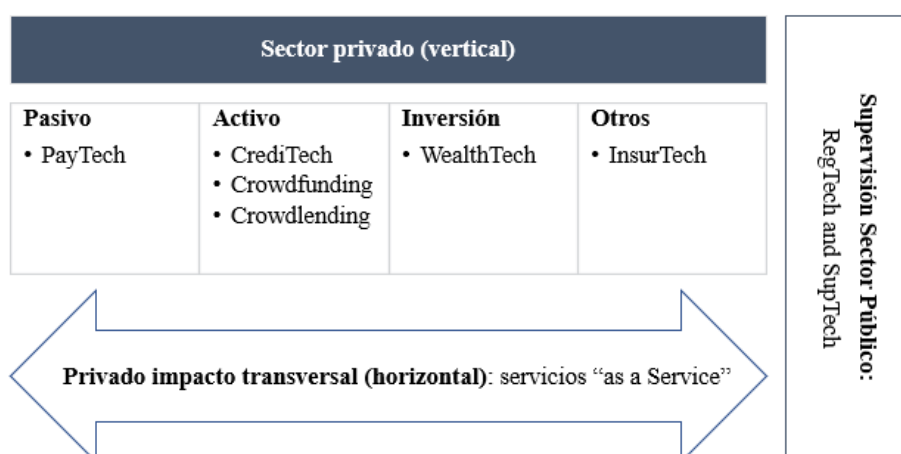


Figura 16. *Ecosistema FinTech 3.0-3.5*

Nota. Elaboración propia.

A continuación, se examina la transformación sufrida en los distintos servicios financieros ofrecidos tradicionalmente al público por parte de instituciones privadas y su supervisión. Con el fin de estructurar el presente trabajo, la transformación del sector privado se agrupó por grupos o verticales de pasivo, activo, inversión y otros. Asimismo, la innovación tecnológica en el sector público se identificó con un único grupo denominado *SupTech*. A estas agrupaciones se les otorgó un carácter de verticalidad en contraste con los modelos que impactan a todos los grupos de forma transversal y que, por tanto, se identificaron como transformaciones horizontales (actividades *as a Service*).

#### **4. Transformación vertical**

La transformación vertical son las actividades *FinTech* que se han especializado o enfocado en un determinado grupo de prestaciones del sector financiero y que, a continuación, se agrupan desde la perspectiva bancaria tradicional; es decir, servicios de pasivo, de activo, de inversión y otros (seguros y auxiliares). A cada uno de estos grupos se les calificó como “verticales”. Debido a la amplia definición de *FinTech*, también se aborda un único vertical de carácter público que comprende las innovaciones tecnológicas en el ámbito supervisor (*SupTech*).

##### ***4.1 Servicios de pasivo y asociados: billeteras, entidades emisoras de dinero electrónico e innovaciones en pagos***

Los servicios de pasivo en banca tradicional por excelencia han sido las cuentas corrientes. Solo aquellas entidades con licencia de entidad de crédito o los establecimientos financieros de créditos están autorizados para la apertura de cuentas corrientes. En el caso español, de acuerdo con el artículo 1.1 de la Ley 10/2014 de ordenación, supervisión y solvencia de entidades de crédito, dichas entidades están capacitadas para recibir depósitos del público y conceder crédito por cuenta propia. Bajo este paraguas se identifican a los bancos, cajas de ahorro y cooperativas de crédito. Ha sido, precisamente este vertical, sus canales y medios uno de los principales impactados por los cambios acontecidos

Con la aparición de la figura de entidades de dinero electrónico (EDE o EMI, por sus siglas en inglés), distintas a las entidades de crédito, fue posible el desarrollo de los conceptos de billeteras electrónicas (o tarjetas monedero) y dinero electrónico. A nivel nacional, dichas entidades están principalmente reguladas a través de la Ley 21/2011, de

26 de julio, de dinero electrónico, y el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico. De este modo, las billeteras electrónicas permiten la acumulación de saldos de dinero electrónico en estas y la realización de pagos, de forma similar a la de una operativa en una cuenta corriente.

En el ámbito público, la Directiva 2009/110/ CE entra a regular el régimen de emisión de dinero electrónico en la zona europea, así como los requisitos que este tipo de entidades deben cumplir para la obtención de su correspondiente licencia. Es precisamente el dinero electrónico lo que permite la figura de las billeteras digitales, abriendo paso a los pagos digitales e incluso el uso de tarjetas virtuales, las cuales permiten prescindir del tradicional concepto de cuenta corriente y, a su vez, que dicho servicio sea ofrecido por otros proveedores de servicios financieros mediante una licencia más liviana, como es la de una EDE.

Las billeteras electrónicas han supuesto un cambio desde la perspectiva de los consumidores finales, permitiendo almacenar valor y transaccionar desde un teléfono inteligente, reduciendo la dependencia del efectivo y del uso de cajeros con sus consiguientes comisiones. Estas se caracterizan por su capacidad de operar de principio a fin totalmente en remoto, es decir, los filtros de conocimiento de cliente se llevan a cabo mediante canales remotos, incluyendo nuevas tecnologías de reconocimiento facial, biometría y prueba de vida para evitar casos de fraude de identidad. Una vez que esos procesos se completan, el contrato de apertura de cuenta, esto es, la solicitud de tarjeta (virtual o física), se lleva a cabo por medio de sistemas de firma electrónica y controles de autenticación de cliente bajo los criterios establecidos por la PSD II. Cuando la apertura se completa, la billetera puede cargarse por distintos medios, tales como ingresos de efectivo en cajeros y establecimientos asociados a la red a la que pertenezca la billetera (denominado *cash in*), transferencia desde otra cuenta o asociación contra una cuenta o tarjeta.

La evolución más sofisticada de las billeteras digitales se encuentra en las billeteras de criptoactivos, que se analizan en detalle en el capítulo de *FinTech 4.0*, y una mejora sustantiva podrá experimentarse una vez los modelos de identidad soberana digital europea planteados en eIDAS 2 sean implementen efectivamente.

Asociadas a las billeteras electrónicas, se presentan nuevas soluciones accesorias de optimización mediante innovaciones de procesamiento que permiten pagos inmediatos, eliminación de pagos entre contrapartes que se encuentren en el mismo entorno operativo

(P2P), NFC o incluso el uso de códigos QR para el procesamiento de pagos. Además, se simplifica la transaccionalidad, al no requerir el conocimiento de los detalles bancarios de la contraparte, lo que permite transferir fondos a una contraparte que sea contacto en la agenda del teléfono y, a su vez, sea cliente de la misma plataforma de pagos (un ejemplo de este tipo de operativas es Bizum). En otros países, estas transacciones también pueden llevarse a cabo con el conocimiento del equivalente al DNI español.

Las grandes empresas tecnológicas han identificado este tipo de negocio como de gran potencial de sinergia con respecto a sus industrias de origen (Barrio, 2021, p. 49). Los ejemplos más claros pueden observarse en la zona asiática, donde el crecimiento de estos sistemas de billeteras de pago como elemento más comprendido dentro de una SuperApp ha sido exponencial.

En el ámbito de la UE, en 2020, el BCE aplaudió la idea de una billetera digital paneuropea, promovida por 16 bancos europeos. En su nota de prensa, el BCE indicó:

*The European Payments Initiative is a response to this call. It seeks to replace national schemes for card, on-line and mobile payments with a unified card and digital wallet that can be used across Europe, thereby doing away with the existing fragmentation. As it is based on the SEPA instant credit transfer (SCT Inst) scheme, it can immediately capitalise onboarding on powerful and sophisticated existing infrastructures, such as the Eurosystem's TARGET Instant Payment Settlement (TIPS).* (European Central Bank (ECB), 2020a, p.1)

Queda por ver el impacto de estos servicios *FinTech* en los bancos, máxime cuando en el marco de un hipotético euro digital se está considerando la posibilidad de contar con este tipo de entidades como participantes en la futura distribución y almacenamiento de las monedas digitales de bancos centrales. Ello se debe a que las billeteras electrónicas vienen a cubrir las necesidades económicas básicas de acceso y uso a medios financieros<sup>44</sup>.

#### **4.2 Servicios de activo**

En lo que respecta a los servicios de activo, la banca ha presenciado a lo largo de los últimos años cómo han surgido nuevos agentes altamente especializados en determinados

---

<sup>44</sup> Recordar Figura 6. Pirámide de necesidades económicas.

nichos que, mediante la aplicación de la tecnología, han logrado aumentar la eficiencia de la operativa y la experiencia del cliente.

La tecnología aplicada a la financiación (*CrediTech*) no solo ha supuesto mejoras de negocios existentes, sino también la aparición de nuevos tipos de servicios (por ejemplo, plataformas de financiación participativa). A continuación, se desarrollan los principales cambios en ambos aspectos, profundizando en el *crowdfunding* debido a que representa un nuevo modelo de financiación que ha requerido de su propia normativa *ad hoc*.

#### 4.2.1 Financiación en línea

El nicho relativo a la concesión de créditos digitales se ha centrado en sus etapas iniciales en el crédito al consumo, entendido como un caso en el que “un prestamista concede o se compromete a conceder a un consumidor un crédito bajo la forma de pago aplazado, préstamo, apertura de crédito o cualquier medio equivalente de financiación” (art. 1.1 de la Ley 16/2011, de 24 de junio, de contratos de crédito al consumo). Sin embargo, ha experimentado un crecimiento exponencial a nivel mundial tanto en términos de volúmenes como de servicios, lanzándose a operaciones de gran valor como las hipotecas (ver Figura 17 ) (García y Natalucci, 2022, pp. 1-4).

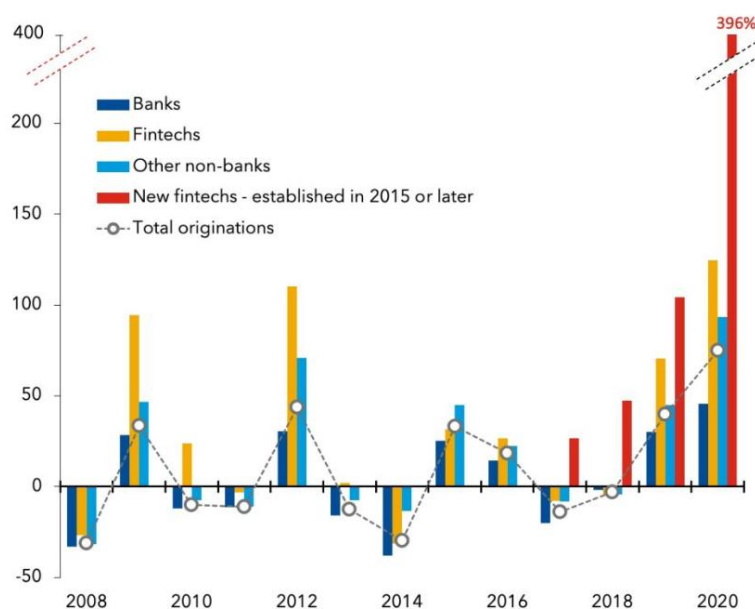


Figura 17. Comparativa de crecimiento interanual en servicios de financiación. La concesión de hipotecas se ha disparado

Nota. Tomado de García, A., & Natalucci, F. (2022). *Fast-Moving FinTech Poses Challenge for Regulators*. IMF Blog: <https://blogs.imf.org/2022/04/13/fast-moving-FinTech-poses-challenge-for-regulators/#>

Como se evidencia en la Figura 17, el mercado de financiación ha experimentado un mayor crecimiento interanual por parte de las instituciones no bancarias y *FinTech*, siendo el mayor crecimiento aquel experimentado por *FinTechs* de reciente creación (de 2015 en adelante), que llegaron a experimentar un crecimiento del 396 % en 2020 según datos publicados por el FMI en su página web (García & Natalucci, 2022, pp. 1-4). Las principales innovaciones de mejora en este campo de créditos en línea han sido la optimización de los análisis de riesgo de crédito que presentan los solicitantes, mediante (i) el perfeccionamiento de la calidad de los datos que nutren los modelos de valoración de crédito, (ii) el uso de nuevos puntos de referencia de datos (nuevos tipos de datos como, por ejemplo, redes sociales) y (iii) el empleo de la ciencia de datos para la creación de algoritmos de puntuación o *scoring*.

De esta manera, el uso de canales totalmente digitales, que abarcan desde la captación y recopilación de información del cliente hasta la evaluación automática del riesgo de crédito y, por tanto, las condiciones a ofertar, permite una clara mejora de la experiencia de usuario mediante una drástica reducción de tiempos hasta la aprobación del crédito. Los servicios de descuento de facturas, adelantos de nóminas y “compra ahora y paga después” también se ven beneficiados por los avances tecnológicos en sus operativas, promoviendo una personalización de tiempos y procesamiento de pagos masivos.

Una transformación del descuento de facturas en línea se produce con el denominado *crowdfunding*, que “permite a las empresas poder adelantar el cobro de sus facturas a través de inversores particulares que adelantan el importe de estas y a cambio obtienen el derecho de cobro al vencimiento de la factura” (AEFI, 2022, pp. 19-20). También surgen soluciones de financiación entre iguales o *peer to peer*, siendo las más conocidas las de *crowdfunding* en sus distintas vertientes (*crowdequity* y *crowdlending*, las cuales se analizan en la siguiente sección).

Con respecto a los créditos digitales es propio de este tipo de modelos *FinTech* el préstamo con recursos propios, debido a que, de este modo, las instituciones quedan fuera del radar supervisor, al menos en España. Sin embargo, existen otras jurisdicciones europeas en las que el requerimiento de licencia no puede evadirse. Ello ha provocado discrepancias en la implantación de la Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, de crédito al consumo en el espacio europeo.

Además, existían elementos de discusión por parte de los jueces, concretamente en casos alemanes como el *Request for a preliminary ruling from the Landgericht*

*Ravensburg (Germany) lodged on 22 January 2021 – VK v BMW Bank GmbH (Case C-38/21)*, en relación con si el derecho de desistimiento del artículo 14.1, que otorga 14 días naturales a partir de la celebración del contrato o desde el día en que el consumidor recibe los términos y condiciones y la información de conformidad con el artículo 10 de la Directiva, podría o no ser invocado de forma indefinida cuando no se haya cumplido con todo lo establecido en el artículo 10 (información que debe mencionarse en los contratos de crédito) (Landgericht Ravensburg, 2021).

La evaluación de solvencia también era un elemento discrepante entre los distintos países de la UE, viéndose agravado a raíz del uso de la tecnología para el diseño de los modelos de valoración no regulados, lo que planteaba cuestiones sobre posibles discriminaciones algorítmicas, falta de transparencia, exceso de uso de datos alternativos y la propia gestión de datos personales (European Commission, 2021d, pp. 1-228).

En general, la directiva de crédito al consumo quedó desactualizada debido a los nuevos modelos de negocio *FinTech* (a modo de ejemplo, no contempla las plataformas de préstamos *peer to peer* en el ámbito o definiciones). Son precisamente los modelos *FinTech* los que plantean nuevos retos materiales no solo respecto a la operativa en sí, sino también respecto a la protección de los consumidores. La COVID-19 agravó aún más el riesgo, dado que las ventas en línea fueron en aumento y, asociadas a ellas, la financiación digital de crédito al consumo (en 2020, el 71 % de los consumidores ya hacía compras por internet) (Comisión Europea, 2021c, pp.1-2).

En consecuencia, en junio de 2021, la CE planteó la revisión de esta directiva en conjunto con la revisión de la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (Comisión Europea, 2021). Esta iniciativa puede resumirse en dos frentes, como describió V. Jourová, vicepresidenta responsable de Valores y Transparencia en la CE:

*Los consumidores se enfrentan a numerosos retos, especialmente en el mundo digital, que ha revolucionado las compras, los servicios o los mercados financieros. Esta es la razón por la que estamos reforzando la protección de los consumidores en dos frentes: facilitamos a los consumidores evitar riesgos relacionados con el crédito y aplicamos normas aún más estrictas en materia de seguridad de los productos. También impondremos una mayor responsabilidad a los participantes en el mercado y dificultaremos que se escondan detrás de una jerga jurídica complicada.* (Comisión Europea, 2021c, pp. 1-2)

En concreto, el documento de evaluación de impacto de la propuesta de directiva de crédito al consumo expone los siguientes objetivos: (i) reducción del detrimento de los consumidores que solicitan préstamos en un mercado cambiante y (ii) facilitar la concesión transfronteriza de crédito al consumo y la mejora de la competitividad del mercado interior (European Commission, 2021d, pp. 1-228). La propuesta se centra en la protección al consumidor, imponiendo nuevas medidas necesarias para los nuevos tiempos, como la exigencia de fórmulas de educación financiera en relación con los riesgos que conlleva el exceso de endeudamiento, los controles respecto a la situación crediticia de los usuarios y la exigencia de que los términos se adapten al uso de nuevos medios como los teléfonos móviles o *tablets*.

Además, adapta los requerimientos de entrega de la información precontractual a los nuevos tiempos, indicando que se debe facilitar con un día de antelación al perfeccionamiento del contrato, con el fin de evitar la contratación impulsiva que genera el uso de medios electrónicos. De no cumplirse, el prestamista debe otorgar al consumidor en las siguientes 24 horas la posibilidad de desistimiento del contrato. También propone soluciones y controles respecto al uso de algoritmos, alineado con la propuesta del Reglamento de Inteligencia Artificial<sup>45</sup>.

Finalmente, se aborda el asunto del control de las entidades no supervisadas mediante la inclusión de un registro y la extensión de los perímetros de supervisión financiera. Esta propuesta regularía casos de préstamos a través de plataformas participativas solo de manera residual, dado que, como se analiza a continuación, estos modelos de negocio disponen de su propia pieza normativa.

#### 4.2.2 Nuevos modelos de financiación: *crowdfunding*

*Crowdfunding*, también denominado micromecenazgo, financiación colectiva, financiación en masa o por suscripción, consiste en la financiación (capital o pasivo) por medio de plataformas digitales, que permiten poner en contacto a los promotores de los proyectos con sus potenciales inversores o prestamistas. En concreto, *crowdfunding* puede definirse como una “actividad de financiación colaborativa y colectiva en la que promotores de proyectos, mediante convocatoria abierta y pública solicitan y reciben

---

<sup>45</sup> Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.



financiación de particulares” (Paredes, 2018, p. 35). Por tanto, se puede hablar de un modelo de base tecnológica y facilitador de desintermediación financiera (Alonso et al., 2020, pp. 621-637).

Tal y como indicó la Dirección General de Tributos (DGT) en su Consulta Vinculante N.º V4050/2015 del 16 diciembre 2015<sup>46</sup>, “Esta institución se caracteriza por la cooperación colectiva, llevada a cabo por personas que realizan una red para conseguir dinero u otros recursos, se suele utilizar Internet para financiar esfuerzos e iniciativas de otras personas u organizaciones”.

El *crowdfunding* se esboza como una suerte de financiación alternativa a la banca, similar a las financiaciones o inversiones llevadas a cabo por las actividades de capital riesgo (Muñoz, 2018, pp. 1-18). Su foco principal son las pymes que buscan soluciones de financiación alternativas o complementarias a la banca. En ese sentido, Muñoz Pérez definió la figura como “medios por el que un grupo de personas o entidades se unen para conseguir colectivizar ingresos y aportaciones para llevar a cabo proyectos comerciales o asociativos” (Muñoz, 2018, pp. 1-18). Esta noción adquirió fuerza en el mundo financiero a raíz de la crisis económica de 2008, en la que los bancos drenaron el acceso a la financiación principalmente de las pymes. De esa manera, surgieron circuitos de financiación alternativos a las instituciones tradicionales, que se denominaron inicialmente como banca en la sombra (Paredes, 2018, p. 20).

Los modelos de *crowdfunding* tienen su origen en un concepto más amplio denominado *crowdsourcing*, que en 2006 se asoció al conocimiento de la multitud o los beneficios que tiene que una función sea propuesta a un grupo abierto de personas para que aporten, reduciendo los costos y sin llegar a ser una tercerización de servicios por completo (Howe, 2006, pp. 1-4).

Respecto a su naturaleza jurídica, debido a que las plataformas de financiación participativa operan como meros puntos de encuentro, se ha llegado a plantear si esta operativa pudiera ser una actividad económica como tal. A este respecto, la DGT, al amparo de la Consulta N.º V2107-18 del 17 julio 2018 esclareció que las plataformas llevan a cabo una carga de trabajo consistente en el análisis económico y financiero de los solicitantes, la monitorización de créditos concedidos, el control y la monitorización de solicitantes y prestatarios, así como la gestión de bases de datos y personal. Por tanto,

---

<sup>46</sup> (DGT, Consulta nº V4050/2015 del 16 de diciembre de 2015, 2015).

la DGT concluyó que se “determina la existencia de una explotación económica que supone la ordenación por cuenta propia de medios materiales y/o humanos con la finalidad de intervenir en la producción o distribución de bienes o servicios”. Se trata, por tanto, de una actividad económica consistente en la oferta de servicios propios de la gestión y coordinación de la plataforma.

Debido a que esta actividad ha requerido del desarrollo de una normativa específica (*ad hoc*) para su seguridad jurídica, merece la pena detenerse a comprender la figura y cómo se ha regulado.

#### **a) Taxonomía de *crowdfunding***

El propio *crowdfunding* aglutina distintas subramas en función de si existe beneficio o no para la plataforma, y del tipo de retorno que tiene la aportación para el individuo que la hace. Sin embargo, existen características comunes, por ejemplo (Rodríguez de las Heras, 2013, pp. 101-123): (i) el empleo de medios electrónicos (plataformas accesibles por vía digital), (ii) el concepto de agrupación o masa (*crowd*) colaborativa, (iii) las operativas *peer to peer* (entre iguales) y (iv) la búsqueda de financiación (*funding*).

Existe una taxonomía generalmente aceptada por los académicos, que divide el *crowdfunding* en cuatro categorías que se explican brevemente a continuación.

La primera categoría es el *crowdfunding* de inversión o *equity crowdfunding*, que consiste en la captación de fondos a través de la plataforma, a cambio de acciones o participaciones de la sociedad promotora. De este modo, los aportantes se convierten en inversores en la sociedad que propone su proyecto.

La segunda categoría es el *crowdfunding* de préstamo, *Marketplace lending* o *crowdlending*. En este caso, el solicitante pide una cantidad en concepto de préstamo, obteniendo financiación que deberá devolverse, por lo general, con intereses. En ese sentido, los aportantes se convierten en prestamistas del solicitante de fondos, que fungirá como prestatario. En función del método de fijación de los tipos de interés aplicables al préstamo, se puede subdividir en fijación mediante subasta o fijación en función de la prima de riesgo (Cuenca, 2019, p. 166).

En ambos casos (*equity* y *lending*), tanto los inversores como los prestamistas están reemplazando los roles de las instituciones financieras tradicionales. La parte de filtrado de la propuesta o análisis de esta es realizada por las plataformas, por lo que no se trata de meros intermediarios, puesto que también tienen funciones sustantivas de control y

promoción sobre los proyectos que se ofertan en sus plataformas (Paredes, 2018, p. 25). Por este motivo, estas dos primeras categorías de financiación participativa se denominan *crowdfunding* financiero, mientras que las dos últimas categorías que se indican a continuación se consideran como *crowdfunding* no financiero.

La tercera categoría (no financiera) sería aquella en la que se propone la puesta en marcha de un producto o servicios (*reward based crowdfunding*). En este caso, el promotor solicita fondos para la fabricación de un producto o puesta en marcha de un servicio. A cambio, los aportantes reciben el propio producto o servicio o descuentos de este, así como otro tipo de beneficios complementarios. Dependiendo de la diferencia entre la cantidad aportada y el valor a cambio, se podrá considerar una compraventa anticipada o una compraventa anticipada más una donación (Camacho, 2018, pp. 43-47).

Por último, existe el *crowdfunding* de donación o *donation based crowdfunding*. Este tipo de *crowdfunding* se realiza con fines benéficos o altruistas, por lo que los aportantes no esperan ningún tipo de recompensa a cambio, existiendo una pura donación (Camacho, 2018, pp. 43-47). Estos casos específicos se encuentran gravados por el Impuesto sobre Sucesiones y Donaciones (BOE de 19 de diciembre de 1987) en cuanto se trata de la “adquisición de bienes y derechos por donación o cualquier otro negocio jurídico a título gratuito e inter vivos”. Debido a ello, se trata de un hecho imponible en el Impuesto de Sucesiones y Donaciones (art. 3.1. b) de la Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones (DGT, Consulta nº V4050/2015 de 16 Diciembre 2015, 2015).

A continuación, en la Figura 18 se observa el árbol de decisión que corresponde a cada uno de los modelos de financiación participativa en función del tiempo que dura la relación entre las contrapartes. En el extremo de corto plazo se encontraría el *crowdfunding* no financiero, en el que no se obtiene nada (donación) o se obtienen pequeñas recompensas a través de los productos o servicios. En el extremo de largo plazo, se encontraría el *crowdfunding* financiero, incluyendo el préstamo que se devolvería a lo largo del tiempo, y, finalmente, el *crowdfunding* de capital social que tiene una vocación de permanencia en el tiempo aún mayor.

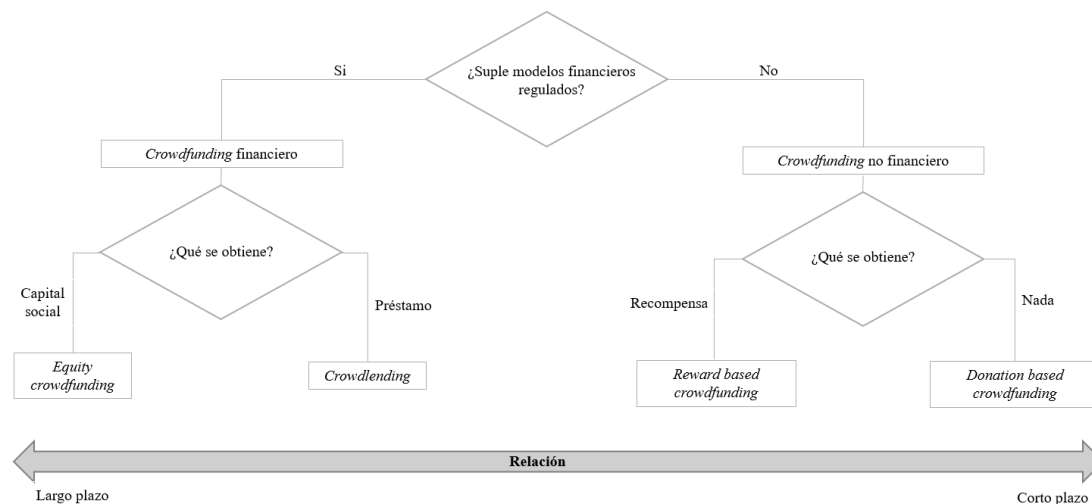


Figura 18. Árbol de decisión de los modelos de crowdfunding en función del tiempo que se mantiene la relación con las contrapartes

Nota. Elaboración propia.

## b) Contrapartes

El *crowdfunding* financiero se concibe como un modelo financiero objeto de supervisión por la UE. Por este motivo, se propuso realizar un análisis de las contrapartes de esta categoría de financiación participativa: promotor, aportante y plataforma.

El promotor es la persona o entidad que presenta el proyecto a la plataforma con el fin de obtener financiación solicitada en nombre propio y abierta del público en general (Rodríguez de las Heras, 2019, p. 113). Este actor requiere de los servicios de la plataforma para el filtro de la solvencia de su proyecto, así como la comunicación y marketing. Está sujeto a controles de diligencia debida por parte de la plataforma.

Los aportantes o financiadores son las personas o entidades que acceden a la plataforma y seleccionan un proyecto en el que aportar fondos, ya sea como inversores o como prestamistas. En este punto, hay que indicar que es común que se realicen inversiones a través de vehículos como pueden ser las gestoras, incluyendo la gestora de la propia plataforma con un límite de hasta el 10 % del objetivo de financiación (artículo 66 de la Ley 5/2015, de 27 de abril, de Fomento de la Financiación Empresarial o LFFE).

Dentro de los inversores, la LFFE distingue entre acreditados y no acreditados, asignando distintos niveles de protección e información a cada uno de ellos. Sin embargo,

el Reglamento (UE) 2020/1503<sup>47</sup> denomina a estos inversores experimentados y no experimentados, cambiando los criterios ligeramente. A modo de ejemplo, en el supuesto de una persona jurídica (empresario), la regulación española requería un balance de al menos 300 000 euros para inversores acreditados (artículo 81 de la LFFE), mientras que el reglamento aminora la cantidad a 100 000 euros. En cuanto a los inversores personas físicas acreditados frente a los inversores personas físicas experimentados, la LFFE requería unos ingresos superiores a 50 000 euros, mientras que el reglamento requiere al menos 60 000 euros anuales, al tiempo que añade nuevos criterios, tales como haber trabajado en el sector financiero por un año, haber estado en un rol ejecutivo en una persona jurídica catalogada como inversor experimentado por el mismo periodo de tiempo o realizar operaciones de volumen significativo bajo ciertos criterios. El reglamento también indica que serán inversores experimentados aquellas personas o entes categorizadas como cliente profesional *per se* bajo el paraguas de MiFID II (Directiva 2014/65/UE<sup>48</sup>).

Finalmente, la plataforma de *crowdfunding* se define en el artículo 46 de la LFFE de 2015 de la siguiente manera:

*Las empresas autorizadas cuya actividad consiste en poner en contacto, de manera profesional y a través de páginas web u otros medios electrónicos, a una pluralidad de personas físicas o jurídicas que ofrecen financiación a cambio de un rendimiento dinerario, denominados inversores, con personas físicas o jurídicas que solicitan financiación en nombre propio para destinarlo a un proyecto de financiación participativa, denominados promotores. (Ley 5/2015)*

Las plataformas de financiación participativa pueden ser de tipo generalista (modelo habitual) o especializadas en determinado tipo de actividades de financiación (por ejemplo, proyectos con fines sociales, como es el caso de la Bolsa Social PFP, S.L. en España).

En general, la plataforma actúa como un intermediario entre las contrapartes anteriormente mencionadas, poniéndolas en contacto. Asimismo, realiza ciertas tareas

---

<sup>47</sup> Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas, y por el que se modifican el Reglamento (UE) 2017/1129 y la Directiva (UE) 2019/1937.

<sup>48</sup> Directiva 2014/65/UE del Parlamento Europeo y del Consejo del 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (refundición) (Texto pertinente a efectos del EEE).

que dan sustancia a su rol y, por tanto, cualifican a este agente como un denominado *gatekeeper*, asignándole cierto tipo de responsabilidades y obligaciones. Entre el rango de actividades que la plataforma puede llevar a cabo, se encuentran las de filtrado de contrapartes, análisis del proyecto (análisis crediticio), comunicación y marketing de este, así como coordinación de los pagos.

A estas tareas, que ya se encontraban reguladas en la ley española, el Reglamento (UE) 2020/1503 añadió un papel similar a la de gestión discrecional de carteras, al incluir la posibilidad de carteras de préstamos, que consiste en la asignación que realiza la plataforma de cantidades determinadas de fondos de un aportante a proyectos de financiación, previo mandato en el que el inversor, de manera individualizada y proactivamente, indica dos de los siguientes condiciones: (i) tipo de interés mínimo y máximo de cada préstamo, (ii) horquilla de fechas de vencimiento de cada préstamo, (iii) gama y distribución de riesgo aplicable a los préstamos y (iv) en caso de que se ofrezca un tipo objetivo anual de rentabilidad de la inversión, la probabilidad de que los préstamos seleccionados permitan al inversor alcanzar el tipo objetivo con un grado de certeza razonable (art. 6 Reglamento (UE) 2020/1503).

En ese orden de ideas, bajo este nuevo tipo de prestación de servicios, la plataforma de *crowdfunding* estará encargada de la evaluación del riesgo crediticio (proyecto, cartera del aportante y promotor del proyecto) y de la provisión de la documentación e información relativa a estos servicios durante la vida de la relación contractual.

### **c) Oportunidades y riesgos**

La financiación a través de *crowdfunding* ofrece ventajas tanto para los promotores como para los aportantes, algunas de las cuales se indican a continuación.

Desde el plano de los promotores, el uso de las plataformas es un trampolín de acceso a aportantes dispuestos a financiar proyectos. Esta capacidad de interacción entre las partes no tiene por qué limitarse al plano financiero, sino que, en ocasiones, los aportantes pueden contribuir con otros elementos de valor como conocimientos especializados (*know-how*) o incluso redes de contactos.

El uso de estas plataformas supone una forma de exposición de la idea al criterio del público no solo como herramienta de marketing (acceso a una masa inicial de potenciales clientes consumidores del producto o servicio), sino también como una forma de validación del potencial interés que el producto o servicio puede levantar de cara a futuras rondas de financiación. Por tanto, el cierre de una financiación por este medio puede servir de indicador positivo para otras contrapartes, como pueden ser ángeles inversores, fondos de capital riesgo o banca tradicional.

Por el ángulo del aportante (prestamista o inversor), las plataformas permiten la contribución a través de cantidades más reducidas de las requeridas en los modelos financieros tradicionales. Además, podrá escoger proyectos a los que se sienta ligado, no solo por elementos financieros, sino también por otro tipo de intereses (el producto o servicio e incluso el propósito del propio proyecto, experiencia en la materia).

En cuanto a los riesgos del *crowdfunding*, de nuevo cabe distinguir entre promotores y aportantes. Los principales riesgos para los promotores pueden dividirse entre legales, estratégico-operacionales y reputacionales.

Entre los denominados riesgos legales se encuentran aquellos derivados de la actividad de acceso a las plataformas por parte de promotores no experimentados. Es frecuente que, debido a su desconocimiento, no cuenten con una idea completa del costo de cumplimiento requerido para el proceso, tanto en términos de tiempo para cubrir los requisitos regulatorios y contractuales (provisión de información, generación de documentos e informes de seguimiento), como financieros (costos legales asociados). Asimismo, se contemplan los riesgos que proceden de la exposición de información al público para obtener financiación, dado que puede generar desprotección de la propiedad intelectual o industrial cuando esta no se haya registrado previamente.

El segundo tipo de riesgos identificados son los estratégico-operacionales, que pueden abarcar un amplio rango de peligros, como, por ejemplo, no conseguir cerrar la financiación, el uso de una plataforma fraudulenta<sup>49</sup> o la propia gestión, transparencia y protección de los inversores (sus expectativas, requerimientos e incluso salidas del capital).

Finalmente, se identifican los riesgos reputacionales. Similar al caso de los riesgos legales, la falta de experiencia de los promotores puede provocar un nivel de calidad inadecuado que sea detectado por los aportantes o la plataforma. Esta impresión negativa puede desembocar en salidas de capital, el veto por parte de la plataforma y, por consiguiente, impactar en futuras fuentes de financiación. En el caso particular de las empresas de capital semilla, este tipo de impacto puede llevar al fin de la vida del emprendimiento.

Por parte del aportante, los riesgos más comunes son de tipo financiero, puesto que las inversiones realizadas se consideran de alta volatilidad. Al igual que con los promotores, también se exponen a que traten con plataformas fraudulentas. Finalmente, a diferencia de otros esquemas, en la actualidad no existen mercados secundarios de *crowdfunding*, por lo que se trata de inversiones altamente ilíquidas, especialmente en el supuesto de *crowdequity*.

También existen riesgos para el sistema financiero en general, debido a la asimetría de la información. En este sentido, las plataformas llevan a cabo análisis de riesgos de crédito, pero carecen de acceso a la Central de Información de Riesgos del Banco de España (CIRBE), puesto que no se consideran entidades financieras. Por este motivo, no acceden a la información respecto al grado de apalancamiento de los promotores. Del mismo modo, las plataformas no reportan las exposiciones de los promotores, por lo que la banca tradicional desconoce el grado de apalancamiento de sus clientes en este tipo de negocios (Cuenca, 2022).

Simplemente hacer un apunte final: el hecho de que las plataformas de financiación participativa se encuentren reguladas y registradas puede, en ocasiones, llevar a la percepción de los inversores de que el nivel de seguridad y garantías de las plataformas es equivalente al de un banco, cuando la realidad no es tal.

---

<sup>49</sup> Se trata de un modelo de estafa en el que la víctima cree estar invirtiendo en proyectos de *crowdfunding*, perdiendo la totalidad de lo invertido. En 2022, la Oficina de Seguridad del Internauta (OSI) alertó de la proliferación de fraudes a través de plataformas de inversión falsas (Biurrun, 2022, pp. 1-5).



#### **d) Comparativa con los flujos operacionales de la banca tradicional**

Los modelos de concesión de préstamos tradicionales pueden dividirse entre la financiación a través de fondos captados del público (ejemplo de concesión de préstamo por una entidad de crédito) o financiación con recursos propios de la entidad (ejemplo de concesión de préstamo por entidad prestamista).

El flujo para estos casos es iniciado por el prestamista (solicitante), quien acude a la entidad. La entidad realiza un análisis desde el punto de vista del cumplimiento normativo (conocimiento de cliente) y también un análisis de riesgo de crédito (impago) debido a que es el banco el que concede el préstamo y corre con el riesgo de crédito (Cuena, 2019, pp. 158-159). Además, no hay conexión directa o contractual entre los individuos que realizan depósitos en la entidad financiera y los que reciben los préstamos por parte de esta. Sin embargo, en los casos de las plataformas de financiación participativa, esta no soporta el riesgo de impago, sino que son los aportantes quienes directamente lo soportan, dado que la relación contractual es directa entre aportante y promotor. La diferencia de flujos puede verse en la Figura 19 a continuación.

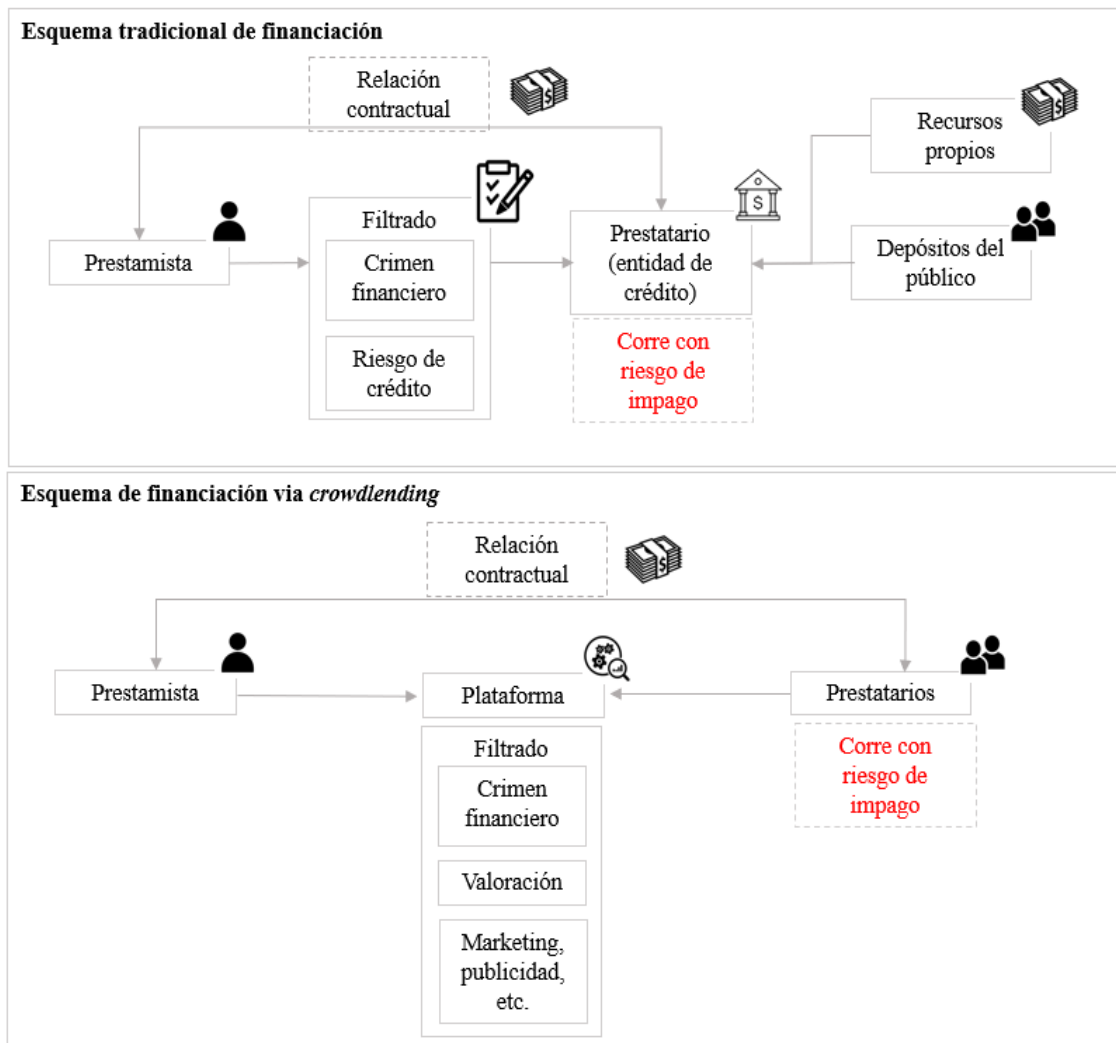


Figura 19. Ejemplo de esquema comparativo de la operativa de financiación en banca tradicional frente a crowdlending

Nota. Elaboración propia, adaptado de *Las FinTech de préstamos o crowdlending. La contratación a través de plataformas intermediarias en línea*, por M.Cuena, 2019, REUS, S.A.

Como se observa en la Figura 19, la relación contractual del esquema tradicional es entre el prestamista y la entidad de crédito, por lo que es esta quien corre con el riesgo del impago. No obstante, en los casos de las plataformas de préstamos participativos, la propia plataforma traslada el riesgo de impago a los prestatarios, puesto que la relación contractual es directa entre prestamista y prestatarios, sin existir un préstamo por parte de la plataforma.

En lo que respecta al *crowdfunding* de inversión o *crowdequity*, este modelo ofrece numerosas ventajas a las contrapartes si se comparan con los procesos de levantamiento de capital tradicionales. En los modelos tradicionales, la operativa práctica se resume en

que la persona o sociedad con la idea debe de contactar uno por uno a potenciales inversores, reunirse con ellos, explicar la idea de negocio y, si resulta de su interés, por lo general, el solicitante debe pasar por el proceso de diligencia debida establecido por cada potencial inversor. Esto se resume en ineficiencias en tiempo y recursos, dado que el solicitante debe tratar a cada potencial inversor por separado, con distintos niveles de requerimientos en cada uno. Además, los inversores pueden ser de distintos tipos, como, por ejemplo, aquellos pertenecientes a su círculo más cercano, ángeles inversores o entidades de capital riesgo.

Las plataformas de financiación participativa de inversión vienen a mejorar la eficiencia de este flujo, centralizando y estandarizando el proceso. La plataforma lleva a cabo los filtros previos de los proyectos en la fase de solicitud por parte de sus promotores. Posteriormente, apoya a los promotores en: (i) el diseño de la presentación del proyecto para potenciales inversores), (ii) la preparación de la documentación soporte requerida en una diligencia debida habitual (equipo, producto, tecnología, proyecciones financieras, capital requerido), (iii) los controles regulatorios de prevención de crimen financiero y prensa negativa, (iv) la publicación y promoción del proyecto en la plataforma y (v) el soporte de formalización de trámites legales y financieros.

De este modo, se reducen las ineficiencias de tener que tratar con distintas contrapartes y requerimientos, así como los tiempos de búsqueda de inversores finales para el cierre exitoso de la operación. Por este motivo, el *crowdfunding* puede concebirse como una herramienta similar al *venture capital*, tal y como apuntó Muñoz Pérez.

#### **e) Ley marco de *crowdfunding*: regulación europea versus regulación española**

En el supuesto de regulación de las plataformas de financiación participativa, España fue uno de los países pioneros de la UE, regulando la actividad mediante la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial y su normativa de desarrollo. La finalidad de la ley no es sino generar un esquema de seguridad jurídica con el fin de potenciar la actividad de plataformas que operen en el territorio español y, a su vez, proteger a los consumidores (Alonso et al., 2020, pp. 623).

El régimen de plataformas de financiación participativa está contenido en el título V de la citada ley, y se estructura en seis capítulos que incluyen la definición y el ámbito de aplicación, los requerimientos de reserva de actividad y los servicios que están

autorizadas a ofrecer normas de conducta, régimen de promotores y proyectos, régimen de protección del inversor y, finalmente, régimen de supervisión, inspección y sanción.

Muñoz, A.F. abordó el título V de la ley, agrupándolo en tres dimensiones, siendo la primera el planteamiento del régimen jurídico de las plataformas de financiación participativa. La segunda dimensión consiste en la reserva de actividad, con el objetivo de dotar al mercado de estabilidad financiera de acuerdo con los principios de proporcionalidad y necesidad del artículo 5 de la Ley 20/2013 del 9 de diciembre (garantía de unidad de mercado). La tercera y última dimensión consiste en las normas que rigen la relación de los agentes que empleen estos servicios (Muñoz, 2018, p.3). Sin embargo, la ley española no deja de ser una solución propia del país, que puede discrepar de las regulaciones o estándares implantados por otros Estados Miembros de la UE, y que genera fragmentación del mercado europeo. En consecuencia, la UE optó por el desarrollo de un reglamento específico en materia de plataformas de financiación participativa con el fin de asegurar un mercado único.

Tal y como se indicó anteriormente, a raíz de la crisis financiera se hizo necesaria la potenciación de fuentes de financiación alternativas, especialmente para empresas de reciente creación o en sus primeras fases de financiación. En 2018, la UE reconoció la falta de un entorno armonizado para este tipo distinto de actividades, indicando que se había llevado a cabo un desarrollo autónomo por parte de ciertos Estados Miembros, pero que no contaba con una base estandarizada de gestión e incluso de régimen aplicable a estas licencias. Esto dio lugar a situaciones de arbitraje y barreras para las *FinTech* dedicadas a estas actividades, por lo que empezó a desarrollar una normativa *ad hoc* a nivel europeo, que permitiera a las empresas de servicios *crowdfunding* operar a través de mecanismos de pasaporte, similar a los aplicados en la banca (European Commission, 2018, pp. 1-18).

Por este motivo, en 2020, la UE publicó el Reglamento (UE) 2020/1503, que se caracteriza por tener una mayor extensión y detalle en comparación con la Ley 5/2015, del 27 de abril. El principal objetivo del reglamento no es otro que solventar la cuestión de la fragmentación de los marcos legales aplicables en la materia para asegurar un adecuado funcionamiento del mercado interior, reforzando la eficiencia del mercado y la protección de los consumidores y usuarios en la UE (Muñoz, 2018, p.11).

El Reglamento (UE) 2020/1503 se caracteriza por introducir umbrales en toda la zona de la UE en términos de importe máximo financiable y límites a la inversión. Asimismo,

introduce la posibilidad de ofertar servicios de gestión discrecional de carteras por estas entidades. También incluye la posibilidad de operar en toda la región mediante el denominado “pasaporte europeo”, que permitirá a las plataformas llevar a cabo estas actividades en todos los Estados Miembros. Finalmente, se incorporan normas de conducta y protección al consumidor.

En lo concerniente a los servicios regulados, existen dos grandes diferencias entre la regulación española y el reglamento europeo. La primera de ellas es el hecho de que el reglamento no permite la inversión propia de la plataforma en los proyectos que ofrece, mientras que la regulación española sí lo permitía siempre y cuando no superara el 10 por ciento. Esto, en la práctica, supone una gran diferencia desde el punto de vista de la entrada de los organismos institucionales o profesionales en las plataformas de financiación participativa. Este tipo de contrapartes, por lo general requieren de cierto nivel de inversión por parte de la plataforma para asegurarse que se ha evaluado el proyecto correctamente, denominando a esta dinámica el “poner la piel en el juego” (*skin in the game*). De este modo, especialmente en los casos de *crowdfunding* de inversión, los organismos institucionales se aseguran de que las plataformas no llevan a cabo una estrategia de negocios cortoplacistas.

La restricción de este tipo de operativa puede suponer la reducción del interés institucional en este tipo de modelos, corriendo el riesgo de ralentizar su crecimiento, dado que este tipo de entidades cuentan con músculo financiero suficiente para impulsar el crecimiento del *crowdfunding* en un corto espacio de tiempo. Por el contrario, el reglamento europeo ofrece una oportunidad de ampliación de nuevas líneas de negocio a través de la gestión individual de carteras de préstamos, que en la normativa española se habían vetado. De este modo, se permitirá la diversificación de fuentes de ingresos.

En lo que al régimen de autorización y operación respecta, el reglamento aborda una problemática constante en los nuevos modelos *FinTech* digitales: cómo gestionar casos en los que las plataformas pueden operar en toda la zona de la UE, con proyectos e inversores de distintos países. A este respecto, se aplica una solución similar al de la banca tradicional, diseñando un sistema de pasaporte europeo con la finalidad de garantizar una adecuada seguridad jurídica en Europa.

Finalmente, el reglamento abre la puerta a lo que parece el inicio de la futura posibilidad del desarrollo de mercados secundarios de *crowdfunding* mediante la publicación en el tablón de anuncios de la plataforma del interés de comprar o vender

préstamos, valores negociables o instrumentos admitidos para la financiación participativa que en un principio se hayan ofertado en la propia plataforma (artículo 25 del Reglamento (UE) 2020/1503). Sin embargo, deja claro que en la actualidad no puede tratarse o asimilarse a un mecanismo de mercado secundario con plena liquidez, puesto que no se permite que la plataforma case intereses de compraventa por medio de métodos o procedimientos internos. Por esta razón, la solución que se ofrece no deja de parecer una solución temporal hasta que el sector adquiriera materialidad suficiente como para requerir la elaboración de una normativa que resuelva esta problemática en profundidad.

En conclusión, si bien es cierto que el reglamento otorga seguridad jurídica, estructura de gobernanza y mecanismos de protección a la clientela, sigue dependiendo de la aplicación local o la interpretación de la norma el éxito o fracaso de este tipo de iniciativas. Además, se eliminan los mecanismos de *skin in the game*, que, si bien reducen posibles conflictos de interés, desincentivan la entrada de inversores institucionales. La solución que se contempla en la ley española, fijando un límite del 10 % parecía ser más adecuada en comparación con el enfoque tomado a nivel región.

Finalmente, en el caso concreto de España, uno de los principales problemas en *crowdequity* es precisamente cómo diseñar vehículos de inversión que faciliten la eficiencia, gestión y futura salida de los inversores.

### **4.3 Productos de inversión**

El ámbito de servicios de inversión es uno de los nichos con mayor potencial de beneficio a través de la aplicación de innovaciones tecnológicas. En esta sección se abordan algunas de las más conocidas, como son el asesoramiento robotizado, *social trading* y *copy trading*, las huchas digitales y el fraccionamiento de instrumentos financieros. Todos ellos buscan reducir las barreras de acceso a este tipo de servicios (ya sea por costos o por perfil de clientes no-objetivo de las instituciones tradicionales).

#### 4.3.1 Asesoramiento robotizado (*robo-advisors*)

La implantación de innovaciones en el vertical de inversión ha sido fruto, principalmente, de la aparición de los denominados *robo-advisors*. Estos programas, que inicialmente realizaban cálculos básicos que permitían la comparación de productos de inversión, han evolucionado hacia programas que permiten la automatización del asesoramiento y las operaciones accesorias a este (Brummer, 2020, p. 201).

Su impulso en la zona europea se debe a los requerimientos de transparencia implementados en especial en MiFID II en su capítulo II, sección II (Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE). Debido a que esta normativa requiere la provisión del detalle de costos y márgenes, la banca de inversión se vio obligada a mostrar este tipo de detalle que, de esta forma, transparentaba al público en general.

Por ello, el cliente podía comparar entre entidades y podía ver los márgenes que las entidades financieras obtenían, provocando una percepción negativa de estas, especialmente en públicos menos sofisticados. Esto, junto con los costos regulatorios que suponían para la banca de inversión, tuvo dos efectos en sus estrategias: (i) la salida de aquellos clientes que no dieran márgenes suficientes, enfocándose en los individuos con altos patrimonios, y (ii) la búsqueda de formas de automatización de los procesos para la reducción de los costos y márgenes. En este contexto, se implementaron innovaciones tecnológicas como reacción a los cambios normativos. En estos casos, el objetivo no es otro que reducir la interacción humana (por tanto, los gastos de filtrado y procesamiento) y estandarizar lo máximo posible para reducir costeos. De esta manera, surgió el asesoramiento robotizado o los *robo advisors*.

Como resultado de la observación antes realizada respecto al enfoque en individuos con alto poder adquisitivo, las empresas *FinTech* identificaron una necesidad no atendida en el resto de los colectivos con cierta capacidad de ahorro, pero menor a los del listón impuesto en la banca. En ese sentido, de nuevo, *FinTech* se presenta como una solución de democratización del acceso a productos financieros (en este caso, de inversión). Sin embargo, estas soluciones no están exentas de elementos de riesgo o preocupación que se exponen a continuación.

Desde el punto de vista de la protección a la clientela, esta democratización implicaba el acceso a productos sofisticados por parte de públicos no habituados o con menos conocimientos de los riesgos que conlleva la contratación de este tipo de servicios. Pese a que MiFID II refuerza e insiste en la necesidad de realizar pruebas de idoneidad y conveniencia, en numerosas ocasiones los supervisores han identificado que estos controles son endeble en su implementación.

Desde el lado de la oferta, la búsqueda de automatización y estandarización en ocasiones ha derivado en la provisión de información cada vez menos adaptada a las

circunstancias específicas de cada cliente (Brummer, 2020, p. 201), reduciendo el margen de interacción humana y, por tanto, la oportunidad de realizar preguntas.

Estos dos elementos han generado focos de quejas y reclamaciones, junto con los ya comentados puntos de transparencia en las comisiones (Comisión Nacional del Mercado de Valores, 2020, p.46). Son precisamente los *robo-advisors*, junto con la oferta de servicios de inversión en criptoactivos, temáticas que ha distinguido la Comisión Nacional del Mercado de Valores (CNMV) como puntos a tratar en su plan de actividades 2021, donde indica:

*Los denominados criptoactivos están captando cada vez más la atención de los inversores y, consecuentemente, de los reguladores y supervisores. En los próximos años se aprobará normativa a nivel europeo para regular este nuevo segmento de los mercados financieros y procurar aprovechar todas las ventajas de la era digital. Además, otros fenómenos como la robotización (robo advisor) o el almacenamiento y tratamiento de datos en la nube también están provocando en nuestro sector cambios relevantes que exigen la atención del supervisor.* (Comisión Nacional del Mercado de Valores [CNMV], 2021, p. 31)

Estos asesoramientos robotizados pueden adoptar dos perspectivas: una de limitación al mínimo de la interacción humana (automatización radical) y otra en la que aún existe cierta interacción con agentes, apoyándose en herramientas tecnológicas para poder proveer sus asesoramientos. En cualquiera de ambos casos, las decisiones se basan en cálculos matemáticos y algoritmos (Tanda y Schena, 2019, p. 19), abriendo la discusión de la necesidad de que estos sean éticamente correctos (no discriminatorios) y quién cuenta con la capacidad de un adecuado diseño y evaluación de estos.

Si bien MiFID II exige un adecuado conocimiento de personas que realizan el asesoramiento o proveen información, la exigencia respecto al diseño de producto no deja claro si los nuevos perfiles, como los desarrolladores, programadores o incluso los ingenieros de datos han de estar sujetos a estos requerimientos o no. Además, estos programas se enfocan en la parte financiera o de oferta del producto, pero no profundizan en aspectos trascendentales como la integridad de la tecnología sobre la que se opera (por ejemplo, *Blockchain*) o los principios que han de regir el desarrollo de algoritmos. Este panorama se hace aún más complejo si se tiene en cuenta que, cada vez con más frecuencia, estas tareas no se desarrollan dentro de las entidades, sino que se realizan mediante la provisión de servicios de terceros.



Por todo lo anterior, se considera que el marco regulatorio actual es insuficiente y no aborda los riesgos inherentes a los que se expone la actividad en la actualidad.

#### 4.3.2 *Social trading* y *copy trading*

La CNMV definió *social trading* de la siguiente manera:

*Plataformas en las que los inversores se ponen en contacto entre sí o con traders profesionales, pudiendo existir diferentes modelos de negocio, que van desde el intercambio de información y opiniones de carácter financiero hasta la emulación de estrategias de inversión de terceros de forma automática.* (Comisión Nacional del Mercado de Valores [CNMV], 2020, p. 110)

Las plataformas de *social trading* permiten a los usuarios interactuar entre ellos, intercambiando opiniones sobre estrategias de inversión (*social trading*). Incluso, estas se transparentan, de tal forma que existe la posibilidad de que otros usuarios puedan replicar o copiar la estrategia de alguien que sea considerado como un experto por la comunidad (*copy trading*) (Rodríguez de las Heras et al., 2019, p- 47). Estos usuarios copiados suelen catalogarse en *rankings* disponibles en la plataforma, donde se suelen mostrar las ganancias obtenidas.

En ese sentido, se denomina *copy trading* a la posibilidad de asignar fondos por parte de los inversores para reproducir las estrategias financieras o posiciones de otro usuario de referencia que también esté en la plataforma (Apesteguía et al., 2019, pp. 1-8). Una vez seleccionado, todas las acciones de inversión o desinversión del usuario de referencia se copiarán proporcionalmente en tiempo real por parte de aquellos miembros de la comunidad que hayan seleccionado la opción de seguir su estrategia. Pese a que la mayoría de los negocios en el contexto de las plataformas de *social trading* están relacionados con operaciones de cambio de divisas, cabe la posibilidad de que se extienda a lo largo del tiempo a otro tipo de productos de inversión como acciones o bonos.

El inversor copiado o *lead investor* suele recibir incentivos o recompensas en forma de descuentos, cuotas o devolución de costos de sus operaciones, dependiendo de la plataforma. Por lo general, la plataforma obtiene sus ingresos de las diferencias de tipos en las operativas (*bid spread*), por lo que su incentivo es aumentar los volúmenes de transacciones dentro de la plataforma (Apesteguía et al., 2019, pp. 1-8).

Pese a la posición de Ballell, que indica que ni la plataforma ni el inversor que es copiado entran en el perímetro del concepto de asesoramiento a la inversión (Rodríguez de las Heras, 2019, p. 47), es claro que se quedan cerca de los límites de este sin que por el momento se hayan tomado decisiones sobre cómo gestionar normativamente estos nuevos modelos de una forma comprensiva. Sin embargo, los supervisores se han pronunciado mediante documentos aclarativos o declaraciones. Ello se debe a que este tipo de modelos ha creado dudas en el público, tal y como captaron las estadísticas relacionadas con el número de consultas recibidas por la CNMV en su portal *FinTech* en 2020, en el que el asesoramiento y gestión automatizadas a través de plataformas de *social trading* se encontraba entre los cuatro principales temas de consulta de los consumidores (Comisión Nacional del Mercado de Valores [CNMV], 2021, p. 326).

En el caso inglés, la UK FCA indicó que los expertos y las plataformas cualifican como sujetos a MiFID II, categorizándolos como *investment manager* o *portfolio manager* (Financial Conduct Authority [FCA], 2016, pp. 1-2). La CNMV adoptó una posición similar al valorar el servicio como de gestión de carteras de inversión (Arias, 2015). Las interpretaciones de la FCA y la CNMV se basan en un documento de la *European Securities and Markets Authority* (ESMA) publicado en 2012, donde aclara este punto en su informe *MiFID Questions and Answers*:

*On the contrary, where no automatic order execution occurs because client action is required prior to each transaction being executed, the activity performed will not amount to portfolio management and, depending on the interaction with the client, other investment services may still be relevant (e.g. investment advice in the case of personal recommendations, and reception and transmission of orders).*  
(European Securities and Markets Authority [ESMA], 2012, p. 15)

Se considera que el *social trading* no entra completamente dentro de esta excepción y, por tanto, la normativa MiFID II le aplicaría. Además, el nivel de conocimiento del inversor que se sigue no es claro, pudiendo haber obtenido ganancias por simple suerte. De nuevo, una excesiva simplificación del proceso (seleccionar la opción de copiar la estrategia), puede llevar a que usuarios con escasos conocimientos estén optando por esquemas de riesgos excesivos de inversión de los que no son conscientes o que no están acordes con el apetito de riesgo que el individuo pueda tener (Apesteгуia et al., 2019, pp. 1-24).

En consecuencia, debería incorporarse la necesidad de crear elementos de control o estandarización por parte de las plataformas enfocadas en dos elementos principalmente: (i) catalogación del nivel de experiencia del usuario copiado (*lead investor*) y (ii) catalogación del nivel de riesgo o exposición que presenta aquella estrategia que se decida seguir o copiar, y contrastarla con un apetito de riesgo que se haya declarado previamente.

Respecto a la catalogación del nivel de experiencia del usuario copiado, como se indicó anteriormente, mostrar solo las ganancias obtenidas puede tener un efecto perverso, puesto que pueden tener su origen en un simple golpe de suerte. En virtud de ello, debería regularse la necesidad de incluir otros elementos en el cuadro de mandos de los expertos, como la coherencia en las ganancias a lo largo del tiempo (por ejemplo, un año o un semestre) o cuánto lleva operando en la plataforma, el nivel de conocimiento en la materia (si es un profesional, si sus estudios están relacionados), el perfil de riesgo de sus posiciones y las inversiones en las que más haya perdido en el último año o semestre.

En cuanto a la catalogación del nivel de riesgo, debería filtrarse previamente el apetito de riesgo de los usuarios. De este modo, si optaran por copiar una estrategia fuera de este apetito, la plataforma debería advertir al usuario de este hecho indicando las posibles pérdidas a las que se expone.

Finalmente, el *social trading* y *copy trading FinTech 3.5* tienen su versión futurista en las DeFi o *FinTech 4.0*.

#### 4.3.3 *Piggy banks* (huchas digitales)

El concepto de *piggy bank* viene a ser la versión digital de la clásica hucha. En este tipo de aplicativos, los usuarios establecen unos objetivos de ahorro en los que, por lo general, se indica el propósito, la cantidad y los tiempos. La intención puede catalogarse en corto plazo (compra de ropa), largo plazo (viaje) o indefinida (incidentes) (De Francisco et al., 2014, pp. 66).

Los fondos pueden ser aportados por la cantidad y periodicidad establecida por el usuario, o también pueden asignarse mediante el método de redondeo. Este método implica que, cuando el usuario realiza una compra en línea por un valor determinado (por ejemplo, una compra por 2,85 euros), los 15 céntimos restantes hasta llegar a los 3 euros se asignarán a la hucha (denominada bóveda o *vault*). Si bien este dinero no figura en la cuenta sino en una sección separada de las aplicaciones, en la práctica se trata de una

mera separación virtual con finalidad puramente psicológica para el usuario, puesto que, si lo deseara, podría emplear esos fondos. Es decir, en la práctica no existe un bloqueo de los fondos en la cuenta, siendo factible disponer de estos.

Los ingresos económicos por parte del banco hucha proviene principalmente de dos fuentes: primero, al incentivar el consumo dentro del comercio electrónico, se reciben comisiones por el uso de tarjetas o por referir a estos clientes; y, segundo, al acumular fondos, se benefician de los depósitos e inversiones intradía que se realizan como parte de la operativa interbancaria (a mayor cantidad, mayor retorno).

Los *piggy bank* o bancos hucha requieren que los fondos se depositen en una entidad regulada y sujeta a supervisión relativa a la gestión de fondos de dinero electrónico. Los nuevos elementos que aparecen están relacionados con combinaciones o derivadas de este modelo de negocio: (i) modelos que apuntan a menores de edad y (ii) modelos que incluyen esquemas de remuneración en cuenta basados en instrumentos financieros y de inversión.

En el primer caso (modelos que apuntan a menores de edad), estas cuentas requieren diligencia debida reforzada, dado que la apertura por menores puede emplearse como herramienta de blanqueo y financiación del terrorismo. Además, los datos de menores están sujetos a requerimientos reforzados conforme al Reglamento Europeo de Protección de Datos (RGPD). La situación se vuelve más preocupante en casos de aplicaciones sujetas a objetos que emplean el IoT para que los padres o tutores premien al menor (este tipo de casos se han desarrollado para promocionar hábitos de ahorro en los menores) (Wei y Lin, 2021, pp. 1-10).

El segundo modelo de esquemas de remuneración en cuenta podría incurrir en requerimientos propios del mundo regulado de inversión, como las licencias, los informes, los requerimientos de transparencia y la protección al inversor que deben tener en cuenta estas entidades.

#### 4.3.4 Fraccionamientos de acciones

Otro de los modelos *FinTech* centralizados que más crecimiento está teniendo es aquel centrado en la democratización de inversiones a través de la compra de fracciones de acciones o instrumentos financieros. Estos modelos pueden considerarse a caballo entre la etapa *FinTech* 3.5 y 4.0, puesto que son originadas por entidades centralizadas que no

son bancos (*FinTech*), pero la tecnología habilitadora o subyacente es la DLT. Debido a que no deja de ser una actividad aún centralizada (CeDeFi), se expone dentro de este capítulo.

Este tipo de soluciones digitales permite que los usuarios creen sus propias carteras de inversión, prescindiendo de las barreras de acceso relacionadas con los precios unitarios de las acciones. Este modelo de fraccionamiento no es sino la creación de derivados sobre el activo subyacente, que es adquirido por la entidad ofertante del servicio. La acción subyacente adquirida por la plataforma es depositada en un banco custodio autorizado y regulado.

Posteriormente, el usuario lleva a cabo una contratación con la plataforma de un derivado representativo del total del subyacente (instrumentos financieros, metales o criptoactivos) o de una fracción de este. En el caso de Bitpanda, estas fracciones se identifican con los denominados *A-Tokens*, que representan las fluctuaciones económicas que va sufriendo el subyacente.

Debido a que se trata de una contratación de derivados, el usuario tiene la capacidad de contratar en cualquier momento, sin estar limitado por restricciones propias de los mercados. Estas contrataciones pueden estar en el Reglamento (UE) N.º 1286/2014 del Parlamento Europeo y del Consejo de 26 de noviembre de 2014, sobre los documentos de datos fundamentales relativos a los productos de inversión minorista vinculados y los productos de inversión basados en seguros, por lo que se ha de presentar un prospecto o documento de datos fundamentales.

Estos modelos de negocio obtienen sus beneficios a través de los *spreads* (Bitpanda Financial Services, 2022, pp. 1-7). Debido a que las acciones subyacentes son propiedad de la plataforma, se hace necesaria la firma de un acuerdo pignoraticio con el fin de devolver a los usuarios el valor equivalente a su fracción de forma preferente en caso de que la entidad entre en quiebra.

#### **4.4 Otros servicios: *InsurTech***

##### **a) Concepto, taxonomía de entidades e innovaciones**

Con base en el concepto de *InsurTech* establecido por la Asociación Española de *FinTech* e *InsurTech* (AEFI) (Asociación Española de *FinTech* e *InsurTech* [AEFI], 2019, p. 18) y ampliando por esta, se puede definir *InsurTech* como el uso de

innovaciones tecnológicas y nuevos modelos de negocio por parte de los participantes en la cadena de valor del sector seguros para agilizar y optimizar el proceso de diseño, distribución y gestión de seguros.

Las entidades que proveen *InsurTech* podrían clasificarse en función de su rol en la cadena de valor (Mueller, 2018, pp. 5-7):

- **Aseguradora completa o *full stack*:** provee el servicio de principio a fin en cuanto a la cadena de valor, incluyendo la captación, contratación y asunción del riesgo.
- **Agentes *InsurTech*:** se trata de aquellas entidades que operan como extensión de la aseguradora y que, por contrato, se les extiende sus obligaciones. Suele asociarse con una aseguradora y pasar por un proceso de autorización de esta.
- ***Brokers InsurTech*:** funcionan como plataformas de agregación y comparación de aseguradoras y agentes. Emplean algoritmos matemáticos para identificar aquellas pólizas que mejor encajen con las necesidades de los clientes. Obtienen incentivos por la generación de oportunidades o *leads*, esto es, referenciar hacia el agente o aseguradora, quienes se encargan de perfeccionar la contratación de la póliza.
- **Habilitadores *InsurTech*:** entidades no reguladas de apoyo interno para soluciones de infraestructura tecnológica, optimización de uso de datos (enfocados a soluciones de explotación de *big data*) o reducción del empleo de personas en tareas administrativas repetitivas.

El sector de seguros es uno de los verticales con capacidad de acoger mayor número de innovaciones tecnológicas para la optimización de su trabajo y el desarrollo de nuevos mercados. A modo de ejemplo, es este vertical uno de los principales potenciales consumidores del IoT (vehículos, inmuebles y *wearables*), así como de *big data* e IA (modelos de riesgos, predicción de demanda y crimen financiero, entre otros).

Innovación	Potencial uso	Mejora
Internet de las cosas (IoT)	Pago por uso (vehículos), datos en tiempo real (salud) para un mejor asesoramiento de riesgos.	Frontales.
<i>Machine learning</i> e inteligencia artificial	Atención y soporte a clientes, procesamiento inicial de quejas y reclamaciones ( <i>chatbots</i> ).	Frontales.
<i>Peer to peer insurance</i> y <i>crowdsurance</i>	Aumento de la oferta en el mercado asegurador. Nuevas formas de negocio.	Frontales.

<b>Innovación</b>	<b>Potencial uso</b>	<b>Mejora</b>
<i>Bots</i>	Automatización de procesos administrativos.	Contabilidad y tareas administrativas
<i>Big data</i> y analítica de datos	Explotación de datos en general. Mejora de los modelos predictivos, ajustes en gestión de riesgos y precios, mejoras en requerimientos relacionados con crimen financiero.	Contabilidad y tareas administrativas
Drones	Asesoramiento remoto en caso de incidente (desastres).	Contabilidad y tareas administrativas
<i>Blockchain</i>	Mejora del procesamiento de las operaciones a lo largo de la vida del seguro.	Contabilidad y tareas administrativas
Enriquecimiento de datos	Mejora de los modelos predictivos, ajustes en gestión de riesgos y precios, mejoras en requerimientos relacionados con crimen financiero.	Contabilidad y tareas administrativas
API	Interconexión segura y automatizada ente entidades.	Contabilidad y tareas administrativas

Tabla 6. *Ejemplos del potencial de las nuevas tecnologías en el sector asegurador*

Nota. Elaboración propia.

## **b) Problemática regulatoria**

Pese a estos avances, el acceso de la innovación aseguradora en la zona europea sigue siendo complicada debido a varios factores. El primero es el hecho de que el mercado de seguros, mediación y distribución está altamente regulado (Directiva 2009/138/UE<sup>50</sup>, Directiva 2016/97/UE<sup>51</sup>, Reglamento de Ejecución (UE) 2017/1469<sup>52</sup>, Reglamento

<sup>50</sup> Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (versión refundida) (Texto pertinente a efectos del EEE).

<sup>51</sup> Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo de 20 de enero de 2016 sobre la distribución de seguros (versión refundida) (Texto pertinente a efectos del EEE).

<sup>52</sup> Reglamento de Ejecución (UE) 2017/1469 de la Comisión de 11 de agosto de 2017 por el que se establece un formato de presentación normalizado para el documento de información sobre productos de seguro (Texto pertinente a efectos del EEE).

Delegado (UE) 2017/2358<sup>53</sup> y Reglamento Delegado (UE) 2017/2359<sup>54</sup>, Ley 20/2015 de 14 de julio<sup>55</sup>, Real Decreto 1060/2015 del 20 de noviembre<sup>56</sup>, entre otros).

Dentro de los requisitos regulatorios, se encuentran los requerimientos de obtención de licencia, los adecuados niveles de capital y la solvencia suficiente para el acceso a la actividad, que claramente no están en la mano de cualquiera y menos de empresas de capital semilla (González de Audinaca, 2019, pp. 104-111). La UE reconoció esta deficiencia y encargó a la European Insurance and Occupational Pensions Authority (EIOPA) la creación de un grupo de trabajo en el contexto del plan de acción *FinTech*. Como resultado, en 2019 se publicó un informe donde se evidencia la existencia de *FinTech* no reguladas en la zona euro y las discrepancias de los países miembros en torno a los enfoques regulatorios de licencias, principios de proporcionalidad y tratamiento de los seguros entre particulares (European Insurance and Occupational Pensions Authority [EIOPA], 2019, pp. 1-40).

En este sentido, la EIOPA realizó una aproximación al uso de innovaciones en el sector tecnológico que se reflejaron en su informe anual de 2020 (European Insurance and Occupational Pensions Authority [EIOPA], 2020, pp. 34-37). Dicho documento, como señaló Tapia Hermida (2021), remarca las dos caras del uso de las nuevas tecnologías y la ciencia de datos. Por un lado, su uso puede facilitar el acceso a los productos, la reducción de precios, las comisiones y los tiempos; pero, por otra parte, su abuso puede llevar a un uso no ético de estos, corriendo el riesgo de generar tratos discriminatorios o abusivos sobre ciertos colectivos o individuos (Tapia, 2021b, pp. 1-7).

Además, las innovaciones que podrían revolucionar el sector, como el seguro de pago por uso (pagar un seguro durante el tiempo que se está alquilando un vehículo), en la actualidad no tendría cabida debido a los requerimientos como el de mantener un seguro durante toda la vida que el vehículo se encuentre estacionado en el territorio (Ley

---

<sup>53</sup> Reglamento Delegado (UE) 2017/2358 de la Comisión de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de control y gobernanza de los productos aplicables a las empresas de seguros y los distribuidores de seguros (Texto pertinente a efectos del EEE).

<sup>54</sup> Reglamento Delegado (UE) 2017/2359 de la Comisión de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de información y las normas de conducta aplicables a la distribución de productos de inversión basados en seguros (Texto pertinente a efectos del EEE).

<sup>55</sup> Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

<sup>56</sup> Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.



21/2007, de 11 de julio, por la que se modifica el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor). Debido a ello, no es posible subdividir o distinguir entre el seguro general del vehículo y el seguro por uso del pasajero o solicitud de mayor cobertura, a modo de ejemplo, en un escenario de uso de un vehículo de transporte con conductor (VTC).

En conclusión, el sector *InsurTech* es uno de los grandes afectados por la falta de regulación de finanzas abiertas que permita seguridad jurídica a sus participantes, pero que, a su vez, aplique un adecuado enfoque basado en riesgos, con estándares homogéneos en toda la zona euro que permitan que aquellas entidades operando con menor materialidad (en volúmenes, operaciones o actividad) puedan estar sujetas a licencias más ligeras e incluso regímenes de simple registro.

Este contexto normativo deberá abordar nuevos casos que han aparecido, como las soluciones enfocadas en la inclusión financiera: los microseguros, el *peer to peer lending* y el *crowdsurance*. Este tipo de productos se han diseñado enfocándose en colectivos de bajo poder adquisitivo o con características que en circunstancias habituales no tendrían acceso a seguros o a rangos limitados de oferta. Por lo general, se suelen centrar en pensiones, vida, accidentes y salud. La operativa suele basarse en un *pool* de asegurados que se unen para tomar la póliza debido a que sus características son similares (AEFI, 2019, pp. 29-33). En ocasiones, este tipo de productos puede ser complemento de otro tipo de iniciativas gubernamentales de microfinanciación o subvención como pueden ser las ayudas en estudios o cosechas (Geczy, 2021).

El desarrollo normativo habrá de profundizar en el área del tecno derecho, puesto que *InsurTech*, al igual que en *PayTech*, implica la desagregación de las actividades en distintos agentes, que deberán de estar conectados entre ellos a través de API que requerirán de normas y estándares de seguridad adecuados para toda la industria. A este respecto, el informe 2020 de la EIOPA también identificó estos fraccionamientos en la cadena de valor mediante la integración con *FinTechs* o *TechFins*, indicando que estos nuevos modelos generan, de nuevo, oportunidades y riesgos no analizados hasta la fecha (Tapia, 2021b, pp. 1-7).

#### **4.5 RegTech y SupTech**

Al igual que el término *FinTech*, no existe unanimidad respecto a la delimitación del término *RegTech*. Teniendo en cuenta la etimología de la palabra (*Regulation/Regulatory*

*Technology*), se puede afirmar que comprende aquellas soluciones tecnológicas enfocadas en aportar cambios materiales en torno al cumplimiento normativo.

La Asociación Española de Compliance (ASCOM) definió el término como “soluciones que utilizan de forma intensiva las “nuevas” tecnologías para facilitar la gestión en *compliance*, simplificando, estandarizando y automatizando los procesos de adaptación a los requerimientos regulatorios, así como los de control y *reporting*” (Asociación Española de Compliance [ASCOM], 2020, p. 2). Por su parte, la European Banking Authority (EBA) lo definió de la siguiente manera: “Any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution (with or without the assistance of *RegTech* provider)” (European Banking Authority [EBA], 2021a, p. 5).

Este sector experimenta su crecimiento por varios motivos, que pueden dividirse en factores desde el lado de la oferta y factores desde el lado de la demanda (Magalhães y Ringe, 2021, pp. 2-3). Desde el lado de la oferta, han surgido numerosos *softwares* de soluciones especializadas en diferentes nichos de mercado o puntos de dolor de sus clientes. Desde el lado de la oferta, la necesidad surge debido al incremento de los requerimientos normativos, su complejidad y su impacto en distintos departamentos o divisiones de la entidad regulada, especialmente en la etapa *FinTech* 3.0-3.5 (por ilustrar, en el sector bancario, en la zona de la UE se solaparon grandes implementaciones regulatorias como MiFID II<sup>57</sup>, PSD II<sup>58</sup>, directivas de prevención de blanqueo<sup>59</sup>, *Foreign Account Tax Compliance Act* [FATCA] y *Common Reporting Standards* [CRS]<sup>60</sup>). Por este motivo, los agentes regulados buscaron soluciones de optimización en términos de tiempo, costo y recursos, identificando *RegTech* como una solución a estos problemas y requerimientos regulatorios. En ese sentido, a diferencia del resto de modelos tecnológicos vistos, la tecnología regulatoria no supone una amenaza a la banca

---

<sup>57</sup> Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (refundición) (Texto pertinente a efectos del EEE).

<sup>58</sup> Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n° 1093/2010 y se deroga la Directiva 2007/64/CE.

<sup>59</sup> Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

<sup>60</sup> OCDE Common Reporting Standards of 15 July 2014.

tradicional, sino que es un elemento complementario de esta, al igual que *LegalTech*, como se verá más adelante.

Inicialmente, este concepto incluyó un subconjunto de actividades enfocadas en la automatización de la supervisión, y que, de acuerdo con su evolución, han devengado en su propia especialidad: la tecnología de supervisión o *SupTech* (Barefoot, 2020, pp. 5-14). Por tanto, se podría distinguir entre la aplicación al sector privado (*RegTech* propiamente dicha, que en ocasiones se denomina *CompTech*, y el sector público (*SupTech*) (European Banking Authority [EBA], 2021a, p. 9).

A la pregunta de por qué los reguladores han de involucrarse en las iniciativas de innovación financiera, la *Financial Conduct Authority* (FCA) ofrece cuatro razones de peso: (i) la promoción de un entorno de innovación seguro favorece la libre competencia de los mercados, otorgando un abanico más amplio de elección a los consumidores; (ii) un mayor conocimiento e involucración en las innovaciones tecnológicas desde una época temprana posibilita al supervisor una mayor previsión estratégica de su potencial impacto; (iii) ligado al punto anterior, un mayor conocimiento de las innovaciones permite asesorar sobre su potencial y los riesgos que presenta; y (iv) la autoinnovación (el conocimiento de estas nuevas herramientas les permite generar nuevas soluciones de supervisión (Financial Conduct Authority [FCA], 2022a, p. 1).

Es precisamente la FCA uno de los reguladores globales más abiertos a la innovación y a la interacción con el sector público. Prueba de ello fue el establecimiento de la función *RegTech* en 2017, y la función de analítica avanzada en 2018 (Financial Conduct Authority [FCA], 2022a, p.1). Esto se ha visto reflejado en sus numerosas y cada vez más frecuentes iniciativas de experimentación con nuevas tecnologías a través de sus *sandbox* regulatorios (financieros y de datos) y otro tipo de llamadas al sector privado mediante fóruns, webinar o *workshops*, además de centros de innovación especializados (ver Figura 20). Ello incluye iniciativas sobre cómo introducir nuevas tecnologías en sus propias dinámicas de trabajo.

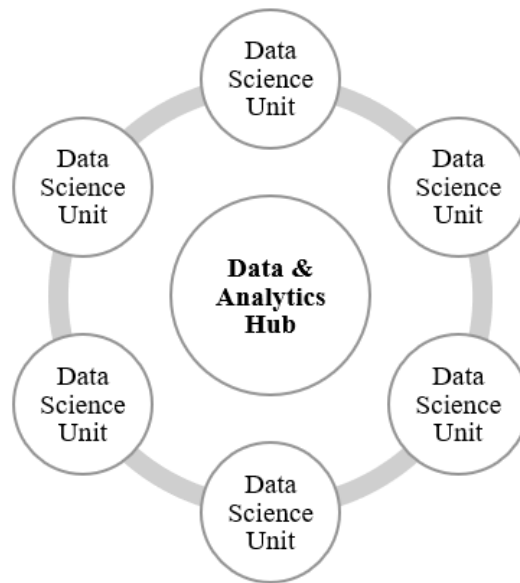


Figura 20. *FCA Data & Analytics Hub: modelo operativo del hub y las distintas unidades de data science*

Nota. Tomado de *Insights from our Approach to Regulatory Innovation. RegTech Forum – Approach to Regulatory Innovation & SupTech*, por Financial Conduct Authority [FCA], 2022a, <https://www.fca.org.uk/events/RegTech-forum-fca-approach-innovation-SupTech>

Testimonio de esta apertura en Reino Unido han sido sus proyectos del FCA Ideas Lab (basado en el *crowdsourcing* de perspectivas de innovación y que generó unas 80 ideas, cuatro de las cuales se implementaron como iniciativas *SupTech* de este regulador). En la actualidad, FCA también está experimentando con la posibilidad de implementar soluciones basadas en tecnologías de la información cuántica (QIT) con el apoyo de expertos académicos (Financial Conduct Authority [FCA], 2022a, p.1).

Asimismo, la operativa del *Data & Analytics Hub* permite a la FCA la adecuada coordinación de las iniciativas de innovación en este organismo, la gestión de contrataciones de perfiles especializados, la puesta en producción de las iniciativas y la formación y mejora de conocimientos internos dentro del supervisor (Financial Conduct Authority [FCA], 2022a, p.1) (ver Figura 20).

En ese orden de ideas, como se puede observar, *RegTech* cubre un amplio espectro de riesgos, tanto públicos como privados, representados por el Milken Institute en la Figura 21, que divide *RegTech* en *CompTech* y *SupTech*. *CompTech* es la tecnología aplicada a cumplimiento normativo en las empresas. *CompTech*, a su vez, incluye monitorizaciones (empleados y riesgos) y remediación (escalado y bloqueo de operativas). Por su lado, *SupTech* incluye monitorizaciones de operaciones irregulares y el análisis de datos. En

un estadio de riesgo mayor, *SupTech* incluye elementos de remediación, como el informe automático o el bloqueo de operaciones automático.

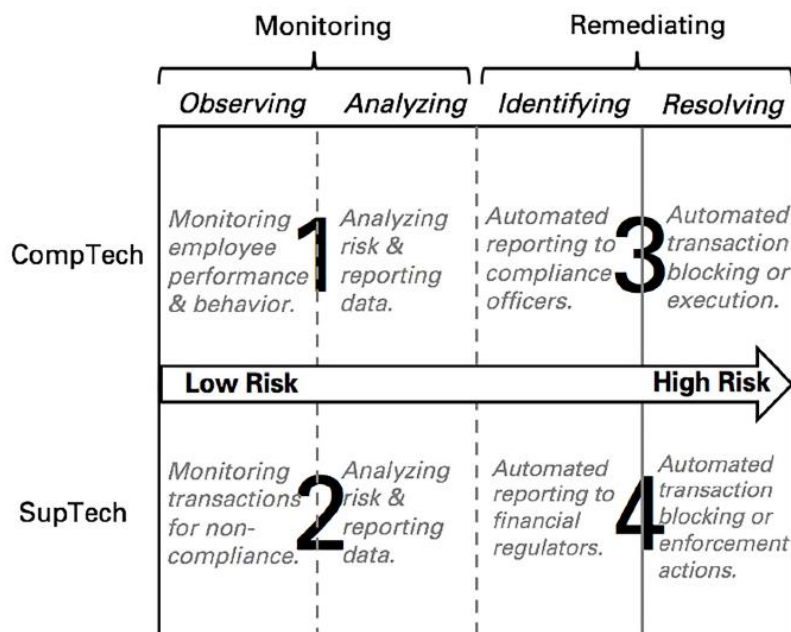


Figura 21. Espectro de riesgos RegTech y niveles de priorización

Nota. Tomado de *RegTech: Opportunities for More Efficient and Effective Regulatory Supervision and Compliance*, por D. Murphy y J. Mueller, 2018, p. 19, Milken Institute.

A diciembre de 2022, el sector *RegTech* no se encontraba regulado en su mayoría. Por este motivo, ha explotado numerosas innovaciones para un mejor desarrollo. Algunos ejemplos de uso tanto en el sector privado como en el público se pueden ver a continuación en la Tabla 7.

Innovación	Potencial uso privado ( <i>CompTech</i> )	Potencial uso público ( <i>SupTech</i> )
Internet de las cosas (IoT)	Seguimiento de mercancías en importación y exportación (prevención de financiación del terrorismo), verificación de que el cliente está vivo (pulso cardíaco en el <i>wearable</i> ).	
<i>Machine learning</i> e IA	Mejora de eficiencia de alertas, análisis de regulaciones, modelos predictivos y de detección de cambios en los mercados, identificación de documentos falsos.	Monitorización de mercados, gestión de datos reportados.
Reconocimiento óptico de caracteres ( <i>Optical Character</i> )	Automatización y relleno de campos de conocimiento de clientes basado en la foto de su documento identificativo, automatización y relleno de campos para análisis de leyes y regulaciones.	Procesamiento de documentación enviada por los sujetos supervisados en formato PDF.

<i>Recognition</i> o OCR)		
<i>Bots y natural language processing</i> (NLP)	Captura y procesamiento de nuevas regulaciones, reducción de tareas administrativas, automatización de informes regulatorios.	Publicación de normativas, reducción de tareas administrativas, automatización de procesamiento de informe (emisión y recepción), recopilación de inteligencia automática (análisis de resultados de Google, noticias <i>online</i> y páginas web). Mejora en la eficiencia de revisión de textos y documentos.
<i>Big data</i> y analítica de datos	Modelos de riesgos de crédito, riesgos de blanqueo y fraude.	Modelos predictivos y de supervisión de los mercados, gestión de datos recibidos. Visualización de interdependencias. Simulación.
Almacenamiento de datos en la nube	Optimización de almacenaje, escalado de capacidad computacional de capturar de datos.	Optimización de almacenaje, escalado de capacidad computacional de capturar de datos.
<i>Blockchain</i>	Procesamiento de soluciones de canales de denuncia y escalado (anonimato, no alteración).	Cambio de infraestructuras, transparencia en asignación de concursos públicos del supervisor, soluciones de canales de denuncia y escalado a autoridades.
Enriquecimiento de datos	Captura de nuevas fuentes de información para mejor perfilado de clientes, contraste de datos provistos por el cliente con fuentes públicas.	Captura de nuevas fuentes de información para detección de potencial prensa negativa de supervisados.
<i>API y data end points</i>	Interconexión y comprobación contra listas de prensa negativa, sanciones, impagos, blanqueo en tiempo real, captura de datos de terceros proveedores que se ponen a disposición de la entidad ( <i>end points</i> ), informes regulatorios.	Informes regulatorios, coordinación entre autoridades, monitorización en tiempo real.
Biometría y pruebas de vida	Verificación de identidad del cliente frente al documento oficial, veracidad del uso en el terminal (teléfono), verificación de que el cliente está vivo.	
Geolocalización	Verificación de que la operativa se lleva a cabo en el país propio del cliente, identificación de retirios en cajeros lejanos a donde el teléfono se encuentra.	

Tabla 7. Ejemplos de innovaciones y su uso en RegTech (sector privado y público)

Nota. Elaboración propia.

Los esfuerzos, análisis, discusión y desarrollo normativo a nivel europeo en temática RegTech se han centrado principalmente en la identidad digital (revisión del Reglamento

eIDAS y el proyecto de Reglamento de eIDAS 2<sup>61</sup>) y la IA (Comunicado de la Comisión Europea sobre inteligencia artificial<sup>62</sup> y el Plan coordinado sobre la IA en 2018<sup>63</sup>, las directrices éticas sobre IA<sup>64</sup> un año más tarde y el Libro Blanco sobre IA<sup>65</sup> en 2020) (Asociación Española de Compliance [ASCOM], 2020, pp. 8-15). Todas estas iniciativas se enmarcan en planes o estrategias generales de la UE relacionadas con la digitalización y gestión de sus riesgos, pero no están dedicadas al vertical financiero en particular. A este respecto, la EBA publicó en 2021 el EBA/REP/2021/17, denominado *EBA Analysis of RegTech in the Financial Sector*.

En conclusión, a diciembre de 2022, el sector *RegTech* no era un sector especialmente regulado, lo que ha permitido proliferar nuevas soluciones de apoyo a los mercados financieros. Sin embargo, se debe tener en cuenta que el aumento del uso de estas soluciones puede suponer una dependencia de los mercados en proveedores de servicios no regulados, por lo que, dependiendo de la materialidad de su rol o función, podrían llegar a catalogarse como proveedores críticos de servicios financieros. Ello implicaría que estas entidades deberían de estar sujetas a controles y supervisión por parte de quienes los contratan. Tal y como lo establecieron las *EBA Guidelines on outsourcing arrangements* (EBA/GL/2019/02), en caso de tercerizar procesos sensibles o críticos, el proveedor de dichos servicios tendría que estar sujeto a diligencia debida por parte de la entidad regulada. Incluso, estas entidades estarían comprendidas dentro de los requerimientos del Reglamento sobre la resiliencia operativa digital (DORA)<sup>66</sup>.

En estos casos, el problema surge de la complejidad de estas tecnologías y no cabe sino preguntarse si el evaluador (la entidad pública o privada que confía en *RegTech*) tiene la capacidad suficiente como para comprender y auditar la tecnología del proveedor *RegTech*. Además, el enfoque *CompTech-SupTech* está tomando una bifurcación de caminos (especialización de soluciones) cuando deberían de tomarse enfoques de

---

<sup>61</sup> Estas regulaciones se analizan más adelante,

<sup>62</sup> Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe COM/2018/237 final.

<sup>63</sup> Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan coordinado sobre la inteligencia artificial COM (2018) 795 final de 7 de diciembre de 2018.

<sup>64</sup> Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019.

<sup>65</sup> Libro Blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza COM/2020/65 final/2 de 19 de febrero de 2020.

<sup>66</sup> Esta normativa se analiza más adelante.

coordinación e interoperabilidad entre las soluciones desarrolladas para el sector privado y público para, de esta forma, optimizar la explotación de las nuevas soluciones y evitar ineficiencias (por ejemplo, soluciones no compatibles o parcialmente compatibles que requieran de revisión u operación manual, incrementando riesgos operacionales o de manipulación). Este enfoque se basaría en una conceptualización de *RegTech* no como soporte a la evolución financiera, sino como un vertical en sí que requiere de su propia reconceptualización.

Esto se complica aún más en lo que, a efectos de esta tesis, se denominó *FinTech 4.0* o el mundo de las DeFi. En estos casos, el rol de *RegTech* es provisto principalmente por la figura de los oráculos y el rol de *SupTech* no se ha definido aún.

## **5. Transformación horizontal: fraccionamientos de la cadena de valor. Proliferación de los negocios “as a Service”**

### ***5.1 Descripción de las actividades***

En los últimos años se ha venido observando una proliferación general de los servicios *as a Service*, que se ha replicado en la industria financiera. En ese sentido, una entidad regulada (por ejemplo, un banco o una *FinTech* regulada) programa la oferta de un nuevo negocio de BaaS, por el que oferta servicios a *FinTech* no reguladas, que operan como frontales tecnológicos de las entidades con licencia.

Estos servicios son de especial interés porque generan una suerte de disfuncionalidad: en la relación interna y forma de ofertar el servicio, es la entidad regulada quien ofrece este a una *FinTech* no regulada que, a efectos de las partes, son sus clientes. Incluso, el servicio se promociona así (BBVA, 2022, pp. 1-6). Sin embargo, desde el plano supervisor, las *FinTech* no reguladas son un agente de la entidad regulada y no un cliente.

La apertura de los datos a terceros y la delegación de cierta operativa de pagos en la banca abierta ha supuesto la disrupción de un mercado tradicionalmente reservado a unos pocos hacia modelos más innovadores y eficientes en costes (Unnax Regulatory Services, EDE, S.L., 2020, pp. 1-10). En este ambiente de banca abierta surgen los modelos de BaaS y FaaS por el que las *FinTech* no reguladas pueden conocer el mercado, acceder y operar, conectadas a través de interfaces de programación, bajo el paraguas de una entidad con licencia que se encarga de supervisar y controlar, corriendo con toda la carga regulatoria.



De esa manera, estos modelos de finanzas *as a Service* afloran como respuesta a estas nuevas necesidades. En ocasiones, pueden verse como el siguiente paso al tradicional concepto de marca blanca que ya se venía empleando principalmente en el ámbito de las tarjetas de crédito, débito y prepago. Sin embargo, se trata de servicios que pueden ser mucho más comprensivos, dado que van más allá de las tarjetas, por lo que la entidad con licencia arriesga más al delegar funciones en un tercero no regulado.

Además, su formato de coordinación y combinación con las entidades financieras con las que colaboran puede ser variado, combinando distintos tipos de servicios (compartir datos, captación de clientes, frontales tecnológicos e incluso agentes o procesadores de transacciones). No solo eso, sino que las plataformas, a su vez, pueden agregar distintos tipos de servicios financieros o incluso híbridos (financieros y no financieros), haciendo que su control y supervisión sea todo un reto (European Banking Authority [EBA], 2021c, pp.10-68). Finalmente, en función de su tamaño, podrán desarrollar ecosistemas en los que la plataforma opere como un *gatekeeper* no solo de datos, sino también de transacciones. A continuación, se muestran dos ejemplos gráficos de modelos operativos de BaaS.

En el primer modelo (integración de una plataforma *FinTech* en BaaS) se puede ver cómo la plataforma opera como frontal tecnológico para un tercero no financiero y para una institución de crédito (formato BaaS), mientras que los pagos pueden llevarse a cabo de forma tradicional mediante cualquier entidad bancaria, puesto que el proceso de pagos se considera secundario (ver Figura 22).

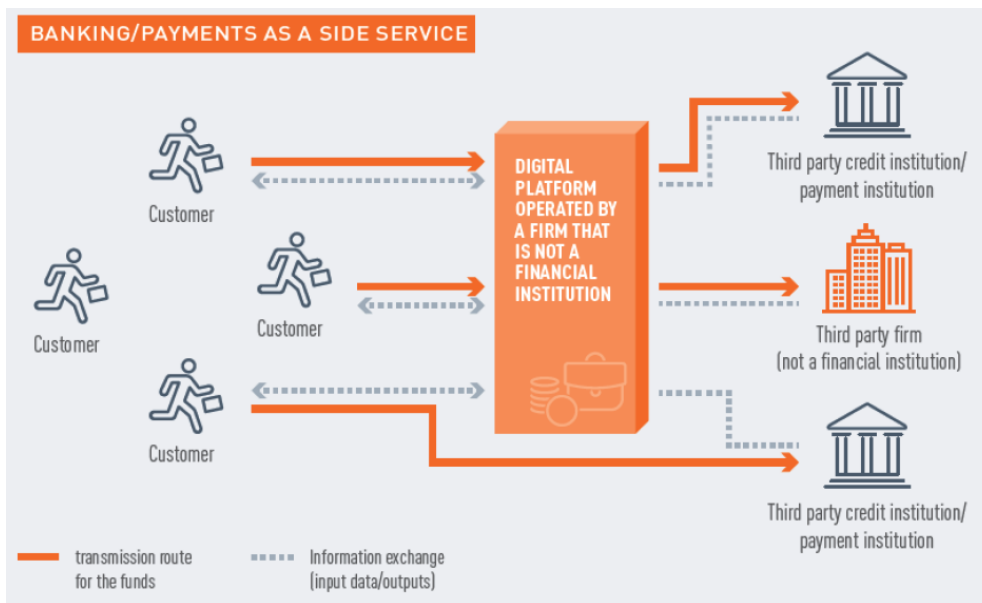


Figura 22. Ejemplo de modelo de integración de una FinTech (Marketplace) en BaaS en el que las operaciones financieras son secundarias o complementarias de las principales

Nota. Tomado de European Banking Authority [EBA]. (2021c). *Report on the use of digital platforms in the EU banking and payments sector. EBA/REP/2021/26. EBA.*

El segundo ejemplo muestra casos en los que el cliente solo interactúa con la plataforma tecnológica, que contiene tanto servicios financieros como no financieros. A su vez, funciona como canal de información y transacción, conectado a terceros no financieros y a entidades reguladas en un modelo de BaaS (ver Figura 23).

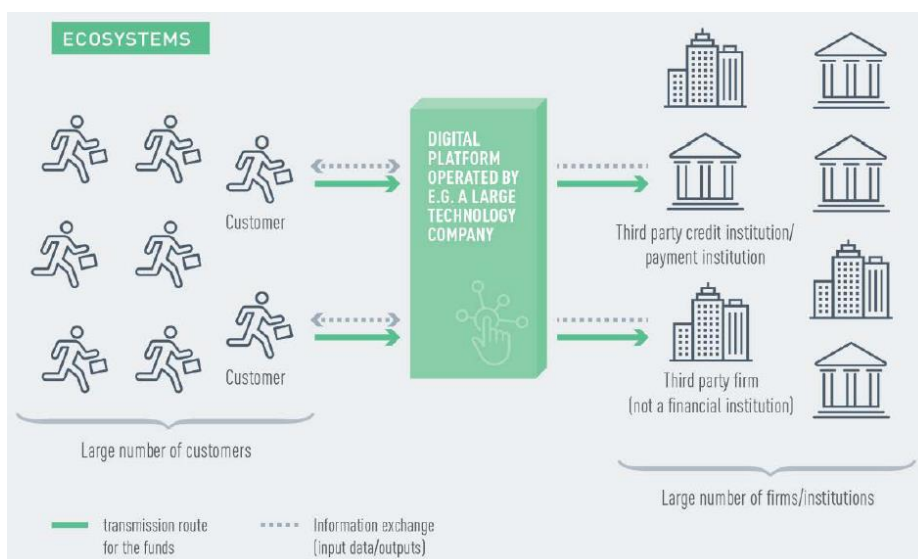


Figura 23. Ejemplo de plataformas operadas por BigTech en las que existe intercambio de información y de transacciones (financieras y no financieras) a través de la plataforma

Nota. Tomado de European Banking Authority [EBA]. (2021c). *Report on the use of digital platforms in the EU banking and payments sector. EBA/REP/2021/26. EBA.*

En esta sección se defiende la necesidad de permitir el progreso de este tipo de relaciones de negocio bajo un panorama regulatorio de mínimos, teniendo en cuenta que este tipo de operativas considerarían a las *FinTech* como proveedores de servicios de las entidades financieras y, por tanto, potencialmente sujetos a los futuros controles bajo el DORA<sup>67</sup>, como se analiza profundidad más adelante. Asimismo, avoca por un enfoque supervisor *ex post* para permitir el avance de la innovación.

En esta sección se analiza cómo operan estos nuevos modelos, cuáles son sus casos de uso, las ventajas e inconvenientes, las perspectivas supervisoras, las implicaciones legales que conllevan para las partes, y se debate si los marcos contractuales en los que en la actualidad operan son adecuados.

## **5.2 Situación actual. PSD II como habilitador**

La banca abierta en Europa ha experimentado un mayor empuje en el sector de pagos a raíz de la directiva conocida como PSD II<sup>68</sup> y todas sus normas de desarrollo. Este contexto normativo otorga seguridad jurídica al mercado europeo, permitiendo que las entidades reguladas del sistema financiero puedan compartir datos de sus clientes y datos de pagos con entidades terceras (conocidas como TPP o *Third Party Providers*<sup>69</sup>).

En ese sentido, bajo consentimiento expreso de los usuarios, se permite el flujo de información no solo relacionada con la identificación y el conocimiento del cliente (comúnmente conocida como KYC<sup>70</sup>), sino también relacionada con la iniciación de pagos o la agregación de datos de cuentas a través de estos terceros.

---

<sup>67</sup> Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011.

<sup>68</sup> Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.

<sup>69</sup> Las TPP en la UE son entidades no bancarias que recaban autorización expresa de los usuarios para acceder a los datos bancarios que estos tengan en una o más entidades financieras o que puedan iniciar pagos.

<sup>70</sup> KYC se refiere al proceso de obtención y verificación de datos identificativos de los clientes requeridos por las regulaciones de prevención de blanqueo de capitales y financiación del terrorismo que estén establecidas por la normativa de las jurisdicciones en las que las entidades operan.

Como consecuencia de ello, emergen las figuras de PISP<sup>71</sup> o agregadores<sup>72</sup> (también denominados AISP), que requieren de licencias más ligeras que las de la banca tradicional, siguiendo el principio de proporcionalidad, y se obtienen en periodos más cortos de tiempo<sup>73</sup>. Por lo general, estos terceros proveedores de servicios suelen ser *FinTech* que entran en el mercado financiero en determinados puntos de la cadena de valor, en los que consideran que están especializados o pueden ofrecer un mejor servicio que la banca tradicional.

Sin embargo, también ha manado una opción secundaria o derivada por la que las entidades reguladas ofrecen sus servicios a *FinTechs* que no cuentan con licencia o están en el proceso de obtención de estas, para que de este modo no pierdan el denominado “*time to market*” o ventana temporal de acceso al mercado. El *time to market* es el tiempo que la empresa toma en lanzar su producto en abierto. Dado que los entornos *FinTech* en estos momentos se mueven a velocidades exponenciales, una idea o producto puede quedarse obsoleto si no se pone en marcha en el momento adecuado. Por lo general, las *FinTech* buscan experimentar, probando si su idea cuenta con el atractivo suficiente antes de plantearse incurrir en costos y cargas regulatorias derivadas de la solicitud de una licencia.

Mientras que Europa evoluciona hacia una mayor apertura de datos relacionados con inversiones o seguros, otras regiones como América Latina han comenzado a tomar pasos hacia estándares similares, encontrándose en distintas velocidades según el país.

#### ***5.4 Las API como elemento clave de estos modelos***

Desde el punto de vista técnico, las entidades reguladas (ya sean instituciones financieras o *FinTech* con licencias limitadas) comparten interfaces de programación de

---

<sup>71</sup> El servicio de iniciación del pago es el “servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago” (artículo 4 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior).

<sup>72</sup> El servicio de información sobre cuentas es el “servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago” (artículo 4 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior).

<sup>73</sup> En el caso de España, la solicitud de autorización debe resolverse en el plazo de tres meses desde su presentación o desde que se complete la documentación necesaria para su evaluación de acuerdo con el artículo 11 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

actividades conocidas comúnmente como API<sup>74</sup> para articular flujos de procesos y modularizar servicios. Las API abiertas suponen una forma de lenguaje y comunicación entre *softwares* que permiten compartir la información de manera prácticamente instantánea (Euro Banking Association, 2017a, pp. 1-33). De este modo, se entregan nuevas experiencias de usuario y existe un margen de evolución alineados con la detección de nuevas necesidades de los clientes o con la aparición de nuevos casos de uso. Esta es la base común tanto del BaaS como del FaaS.

En ese sentido, a diferencia de las operativas previas a la PSD II, las API abiertas posibilitan la interconexión entre distintos participantes, facilitando al usuario final una mejor gestión de la información y, por ende, una optimización de su proceso de toma de decisiones (ver Figura 24). Efectivamente, tal y como muestra la figura, el cliente no tendrá la información fraccionada en la aplicación de cada banco, sino que podrá contar con una sola aplicación o web que reúna la información de las cuentas corrientes de todos los bancos e iniciación de pagos (bajo modelo de banca abierta) o incluso la información, comparación, contratación o iniciación de operaciones de tipo financiero en general en finanzas abiertas, permitiendo una mejora en la toma de decisiones y gestión.

---

<sup>74</sup> “Las API son interfaces entre aplicaciones de *software*, que se aplican tanto dentro de las organizaciones como entre organizaciones. Más específicamente: las API permiten la comunicación entre aplicaciones de *software* donde una aplicación llama sobre la funcionalidad de otra aplicación” (Euro Banking Association, 2017a, p. 2).

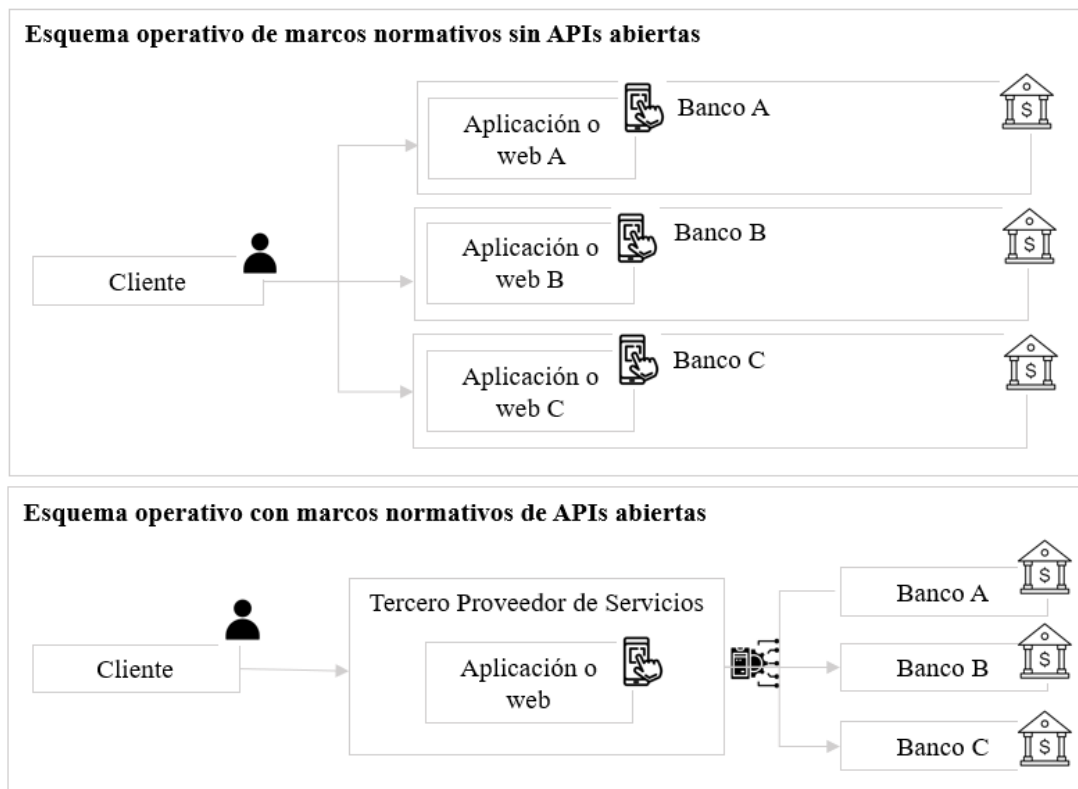


Figura 24. Ejemplo comparativo de los modelos operacionales previos a la implementación de normativas de API abiertas y posteriores a esta

Nota. Elaboración propia.

Es importante destacar que, en estos modelos centrados en las API, la documentación de estas y los requerimientos técnicos relacionados juegan un papel clave, por lo que las instituciones reguladas deben contar con la documentación actualizada y los flujos de notificación de actualizaciones eficientes (por lo general, disponibles en los portales para desarrolladores).

Podría considerarse que estos modelos son similares a una externalización de servicios tecnológicos y, por tanto, asimilarse a estructuras contractuales ya existentes; sin embargo, pese a que hay elementos comunes, se debe tener en cuenta que en los modelos BaaS y FaaS los niveles de estandarización y automatización de los módulos o servicios ofrecidos es mucho mayor. La intervención humana o la delegación de personal técnico de una entidad a otra se reduce drásticamente o es inexistente (Perc y Forst, 2017, pp. 1-20).

## 5.5 *Banking as a Service*

BaaS aporta valor incremental a las contrapartes (entidad regulada, *FinTech* y consumidor final). La principal razón es que se basa en un modelo de colaboración de la banca con las *FinTech* (confianza, generación y uso de datos), lo que permite al usuario final tomar decisiones más completas debido a la mejora en términos de tiempo y calidad de los datos.

El ofrecer BaaS por parte de instituciones financieras debe ser una decisión estratégica, puesto que implica una apertura del banco hacia terceros, que requerirá de una evolución y que conlleva varias fases (desde el análisis de potenciales colaboradores para pilotos, desarrollo de portales API para desarrolladores o cambios en las arquitecturas de sistemas hasta cambios en las jerarquías y tiempos de toma de decisiones que permitan implementaciones en semanas o días) (Cognizant, 2016, pp. 1-20).

El BaaS parte de la idea de un *modular banking* (Asociación Española de *FinTech* e *InsurTech* [AEFI], 2020, pp- 1-77) (similar a las piezas de los legos), cuyas partes o módulos pueden reutilizarse fácilmente a través de API (servicios conocidos como *plug and play*) (Cognizant, 2016, pp. 1-20). Por este motivo, no existe un modelo único de BaaS, sino múltiples, que pueden tener distintos niveles de granularidad.

La oferta de servicios BaaS puede ir desde la contratación de un servicio en particular (por ejemplo, emisión de tarjetas o un módulo de *rating* de créditos) hasta un servicio similar al de llave en mano en el que se ofrecen todas las utilidades en una oferta de marca blanca (se muestran logos de la *FinTech* y solo la documentación legal muestra referencias al socio financiero) o *cobranding*<sup>75</sup> (a lo largo de todas las pantallas y operativas se muestran logos de la *FinTech* y la entidad financiera con la que colabora, ofreciendo una mayor transparencia al público final). En consecuencia, este tipo de activos *as a Service* puede ser muy variado y modular, incluyendo diversos elementos que pueden añadirse o no en función de las necesidades y la evolución de la relación.

Las contrapartes o consumidores de estos modelos BaaS pueden ser otras instituciones financieras (generalmente más pequeñas, menos desarrolladas), entidades con licencias más ligeras (PISP o AISP, en el caso europeo), *FinTechs* (reguladas, en proceso de

---

<sup>75</sup> En este caso específico, el *cobranding* consiste en la unión pública de dos marcas (una regulada y otra no regulada) con el fin de presentar al público un nuevo producto o servicio, mostrando a los usuarios dicha colaboración de manera transparente.

obtención de licencias o no reguladas) o terceros no regulados (desde plataformas tecnológicas provenientes de otros sectores hasta aerolíneas) (Capgemini, 2021, pp. 3-34).

El resultado final tipo para el usuario es una aplicación de servicios financieros ofrecida por un frontal tecnológico que se asimila a un banco. Sin embargo, legalmente, estas entidades carecen de licencia o cuentan con una licencia limitada (caso de neobancos), y suelen ser agentes o comisionistas mercantiles de entidades reguladas (son una plataforma donde se incrustan microaplicaciones de entidades reguladas o no, convirtiéndose en plataformas de oferta de servicios financieros o incluso plataformas de servicios híbridos – financieros y no financieros).

Para llegar a este objetivo de la forma más liviana posible, la cadena de valor se fragmenta en diversas contrapartes especializadas, llevando a cabo tercerizaciones de distintos módulos (regulados o no). La infraestructura tecnológica replica estas fragmentaciones y se conecta con estos terceros proveedores de distintos servicios (ver Figura 25). Como muestra la Figura 25, puede existir una entidad *FinTech* (no regulada) o regulada parcialmente (neobanco) operando como frontal tecnológico de cara a los usuarios, que cuente con un sistema cuya infraestructura sea propia o incluso de un tercero. Por otro lado, establece relaciones contractuales con marcas (Visa, Mastercard, Union Pay, American Express, entre otras), procesadores de tarjetas y otros proveedores de servicios que se integren en la plataforma. Los servicios financieros y acceso a las cámaras de compensación y liquidación se obtienen a través de una entidad financiera regulada, mediante un acuerdo de colaboración en formato de agencia o comisionista.



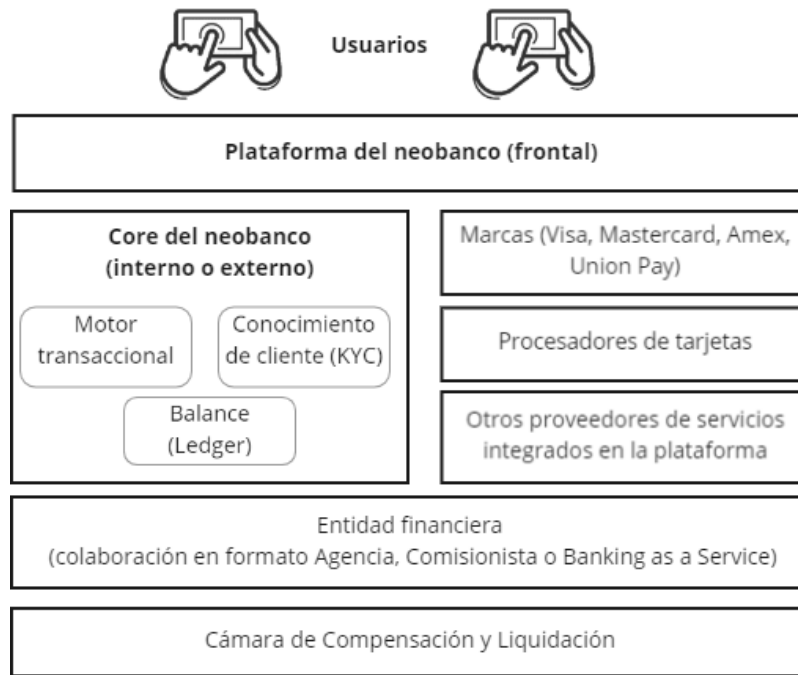


Figura 25 Ejemplo de infraestructura tecnológica en modelo Banking as a Service de un neobanco

Nota. Elaboración propia.

La fragmentación de las cadenas de valor en servicios financieros presenta diversos retos a los reguladores y supervisores, puesto que las tercerizaciones pueden ser a entidades bajo su supervisión o no, a países terceros equivalentes o no, presentando, por tanto, nuevos riesgos a explorar.

La situación se complica más aún si se observa que los neobancos que consumen estos servicios de forma total o parcial, los reagrupan y combinan con ofertas de valor no relacionadas con servicios bancarios, pero complementarias con los públicos a los que se dirigen. En ese sentido, no queda claro qué servicios de los ofertados están bajo el perímetro de supervisión y cuáles se quedan por fuera. Tampoco es fácil identificar cuáles son productos propios de la plataforma y cuáles son ofertados por terceros.

De manera similar, a nivel mundial, la estrategia de *BigTechs* (Gorjón, 2021) en la zona occidental (por lo general más regulada) han sido modelos de colaboración de este tipo con bancos, permitiendo servicios complementarios a los ya ofrecidos en un plazo corto de tiempo, sin tener que esperar a la obtención de licencias formales que pueden llevar más tiempo que las de los países asiáticos, donde existen distintos niveles o tipos de licencias, como las específicas de bancos virtuales.

## 5.6 FinTech as a Service

El FaaS se da en los casos en los que las entidades *FinTech* con licencias limitadas (por ejemplo, emisores de dinero electrónico, iniciadores de pago o agregadores) abren líneas de negocio encaminadas a la oferta de API propias a terceros no regulados. La contraprestación por estos servicios puede venir en forma de comisiones o mediante la obtención de datos (la nueva moneda de cambio de la era digital). Esta nueva tendencia es aún más reciente que el BaaS y, por tanto, aún no está regulada en muchos países, por lo que adolece de un mayor nivel de inseguridad jurídica y es aún más desconocido por los reguladores.

Además, en estos casos, las cadenas de valor pueden llegar a ser aún más fragmentadas o complejas desde el punto de vista operativo-tecnológico, puesto que, por lo general, las *FinTech* con licencia suelen tener limitaciones. Entre estas limitaciones, una de las principales es que las *FinTech* reguladas no suelen ser miembros de las cámaras de compensación y liquidación electrónica de los países. De este modo, para completar sus operativas, requieren de una institución financiera (por lo general un banco) que sea miembro directo de la cámara de compensación y liquidación, añadiendo al menos un componente más a estos legos financieros (ver Figura 26).

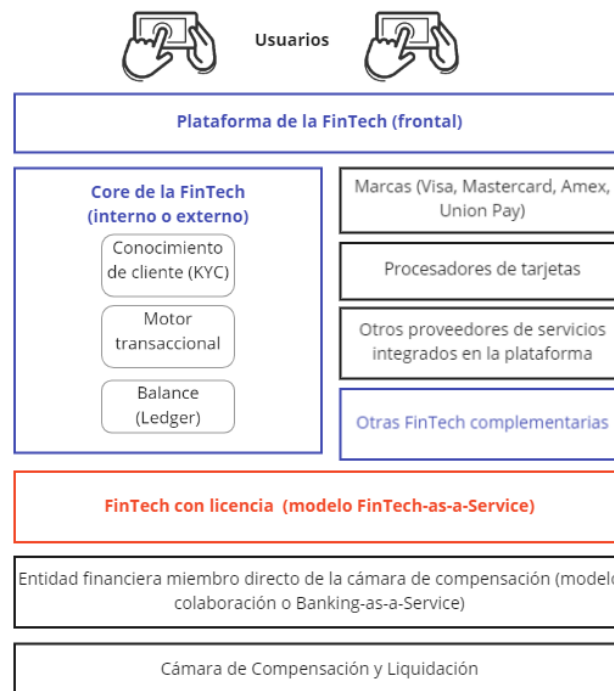


Figura 26 Ejemplo de infraestructura modular en el FinTech as a Service de pagos

Nota. Elaboración propia.

## 5.7 Oportunidades

Para las entidades reguladas (ya sean instituciones financieras o *FinTech* con licencias más ligeras), este nuevo modelo de negocio representa una nueva fuente de ingresos (Accenture, 2014, pp. 1-2) y una forma de monetización de las estructuras tecnológicas, operativas y de cumplimiento normativo con las que ya cuentan. De esta forma, las entidades reguladas pueden diversificar sus negocios (Capgemini, 2021, pp. 3-34) y supone una forma de evolucionar al ritmo del mercado sin tener que incurrir en grandes inversiones debido a la necesidad de cambios derivados de sistemas heredados.

En países emergentes, estas soluciones permiten que las instituciones financieras que hasta el momento no hayan llevado a cabo desarrollos de negocio a distancia, puedan encontrar socios que funcionen como sus frontales tecnológicos y les permitan una captación de público al que hasta ahora no habían llegado.

La banca tradicional puede considerar este marco contractual como una oportunidad de captación de clientes que para la propia entidad no habían resultado rentables hasta el momento (Capgemini, 2021, pp. 3-34), por lo que podría abrir el foco en nuevos colectivos. Se ha de considerar que las *FinTech* permiten automatizaciones de procesos, reduciendo costos y, en ocasiones, cuentan con soluciones que permiten el enriquecimiento de datos relativos a clientes con los que la banca podría no contar o incluso el ofrecimiento de nuevos productos y servicios (Cognizant, 2016, pp. 1-20). De esta forma, estos modelos de colaboración pueden abrir el acceso a servicios financieros a colectivos no bancarizados o sub bancarizados, suponiendo una oportunidad para la inclusión financiera en los países emergentes.

Del otro lado de la moneda, las *start-ups* entrantes consumidores de estos modelos se apalancan en socios regulados con estructuras ya establecidas, evitando incurrir en desarrollos internos que puedan ser excesivamente onerosos para la etapa en la que se encuentran, permitiéndoles enfocarse en su propuesta de valor y elementos diferenciadores de cara a clientes (Accenture, 2014, pp. 1-2). De este modo, experimentan y conocen el mercado en el que entran con antelación, bajo un entorno de seguridad ofrecida por el control de una entidad regulada.

Esta simbiosis entre ambas partes permite que los bancos conozcan nuevos modelos o ideas de mejora de carácter eminentemente tecnológico de los que ellos no sean expertos o no puedan desarrollar debido a sus legados de infraestructuras tecnológicas. Las

*FinTech* aprenderán los estándares regulatorios y de control de los países de la mano de sus *partners* financieros regulados antes de comenzar su andadura de forma totalmente independiente.

Los modelos de BaaS y FaaS se han extendido principalmente a los subsectores de pagos y préstamos. En el caso concreto de los préstamos, los bancos han ofrecido este servicio a *FinTech* de créditos (*CrediTech*) que cuentan con desarrollos tecnológicos que permiten automatizaciones robóticas de procesos (*Robotic Process Automatization* o RPA, por sus siglas en inglés) y de gestión y análisis documental de *onboarding* para descargar a sus comerciales de tareas administrativas y poder centrarse en operaciones más complejas o de mayor valor añadido (Finezza, 2020, pp. 1-6).

## **5.8 Problemáticas que plantean**

### 5.8.1 Desde el punto de vista de las políticas públicas de supervisión

Debido a lo novedoso de estas nuevas pautas de negocio, aún existe poca o ninguna regulación dependiendo de la jurisdicción, por lo que la inseguridad jurídica es mayor. Asimismo, se trata de casos en constante evolución, que aún no son del todo conocidos por los reguladores de países emergentes, por lo que existe el riesgo de que intenten encajarse en modelos contractuales no adecuados o incluso se prohíban.

Dependiendo del país, la entidad regulada tendrá la obligación de notificar o solicitar aprobación de esta delegación de funciones a los supervisores. El régimen de simple notificación parece ser el más apropiado para estas circunstancias siempre y cuando no se trate de un servicio integral, puesto que permite mantener la rapidez y flexibilidad necesaria.

Con posterioridad, las autoridades podrán solicitar información con el fin de evaluar si los controles que la entidad regulada ha impuesto a su agente o comisionista en el modelo de BaaS o FaaS son adecuados. De esa manera, el negocio puede seguir la velocidad que requiere este tipo de mercado, dentro de un ambiente de control adecuado. Los supervisores pueden llegar a entender estos modelos como un vaciado, cesión o renta de licencia, sin tener en cuenta el componente de modularidad, corriendo el riesgo de prohibir estos modelos puente y, por tanto, limitando el acceso al mercado e innovación. Tal es el caso mexicano, que en diciembre de 2020 emitió un aviso público indicando lo siguiente:

[...]las autorizaciones otorgadas a entidades financieras son intransferibles, ninguna ley financiera autoriza a ceder, rentar, prestar o de cualquier forma compartir su licencia o autorización, por lo que no puede usarse una licencia por un tercero para ofrecer, promover o prestar servicios financieros de forma directa (sin ser comisionista o representante legal). (Comisión Nacional Bancaria y de Valores de México [CNBV], 2020, pp. 1-3)

De este modo, pese a que el país había establecido las bases del *open banking* en 2018<sup>76</sup> y 2020<sup>77</sup>, parece que limita el FaaS al modelo del comisionista mercantil con los requerimientos correspondientes al *outsourcing* tradicional, requiriendo evaluación y aprobación por el supervisor. Además, no espera desarrollar modelos contractuales *ad hoc* para estos casos que encajen mejor con los nuevos modelos y ofrezcan un enfoque basado en riesgos en función del tipo de servicio o módulo que se requiera.

Como ya se había comentado, resultado de la fragmentación de las cadenas de valor, los supervisores pueden verse tentados a extender sus mandatos hacia aspectos más tecnológicos que financieros, debido a que los límites entre industrias se están desdibujando y las contrapartes que pueden presentarse como meros proveedores tecnológicos resultan ser clave para estos nuevos modelos bancarios desagregados.

En países en los que las regulaciones de banca abierta están en fase de desarrollo o aún no se han planteado y el nivel de inseguridad jurídica es mayor, requiriendo de interpretaciones de marcos normativos que el regulador no ha llevado a cabo, teniendo en cuenta estos avances en modelos colaborativos de entidad regulada-tercero no regulado. Es decir, en estos casos, es el supervisor quien está aplicando soluciones técnicas de analogía a la espera de soluciones estratégicas de desarrollos regulatorios. En este contexto, es recomendable obtener el apoyo de las autoridades para conocer su grado de apertura a reinterpretaciones de la normativa existente con el fin de dar cabida a estos nuevos modelos dentro de los rangos regulatorios existentes.

---

<sup>76</sup> La Ley para Regular las Instituciones de Tecnología Financiera se publicó en el Diario Oficial de la Federación (DOF) el 9 de marzo de 2018.

<sup>77</sup> Disposiciones de carácter general relativas a las interfaces de programación de aplicaciones informáticas estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera publicada en el DOF el 4 de junio de 2020.

## 5.8.2 Desde el punto de vista de encaje contractual

En los supuestos de *BaaS* y *FaaS*, las *FinTech* interesadas en probar sus modelos o comenzar a operar, articulan contratos de colaboración, comisión mercantil o agencia con las entidades reguladas que extienden la cobertura de sus licencias a estos terceros no regulados. Debido a que las entidades con licencia delegan funciones críticas generalmente, estos contratos deben venir acompañados con acuerdos de niveles de servicios (SLA) que detallen los flujos operativos, las horas de servicio operativo, los requerimientos tecnológicos, los roles y las responsabilidades de las partes, las obligaciones de escalados de incidencias, los planes de contingencia y los derechos a la realización de auditorías periódicas por parte de la entidad regulada.

Los SLA buscan detallar las expectativas de cada una de las partes respecto a los servicios que se proveerán, niveles de calidad y tiempos de respuesta (Jin, Vijay, & Akhil, 2002, pp. 1-13). En virtud de que se trata de modelos de negocio jóvenes en constante evolución, aún no existen estándares mínimos en la industria en relación con estos modelos contractuales y sus anexos. Este tipo de contratos también deberá contemplar los principales criterios o mitigantes de los riesgos que estas operativas pueden conllevar, especialmente en términos de prevención de blanqueo de capitales y financiación del terrorismo, protección de datos, ciberseguridad, tercerizaciones y asuntos de transparencia y protección al consumidor (European Banking Authority [EBA], 2021c, p. 44).

El propio modelo de agente o comisionista parece ser inadecuado si se analiza la finalidad y la relación real entre las partes: la finalidad última de la entidad no regulada consiste en entrar en el mercado, operar y adquirir clientes; sin embargo, bajo estos modelos, son meros agentes o comisionistas y los clientes son de la entidad promotora del BaaS o del FaaS. Una vez la entidad no regulada obtuviera los permisos, no sería factible una migración de clientela, dado que esta nunca ha sido propia, sino de la entidad con licencia.

Por otra parte, como se indicó, la fragmentación de la cadena de valor de la oferta de servicios financieros genera nuevos riesgos si se tiene en cuenta que parte de esas tercerizaciones es a entidades no reguladas (por lo general de perfil tecnológico), desconocedoras de controles relativos a cumplimiento normativo o al negocio de la banca. En un entorno cada vez más global, pueden darse casuísticas de servicios en la nube, por

lo que pueden darse casos de transferencias de datos a países terceros no equivalentes. Además, en el caso de las entidades tecnológicas, el uso de subcontrataciones o contratación de desarrolladores bajo acuerdos de *freelance* es habitual, por lo que la entidad promovente del BaaS o FaaS deberá establecer requisitos de control al respecto (desde prohibiciones o limitaciones hasta formaciones periódicas a los encargados del proyecto común).

Dado que se está hablando de formas de negocios jóvenes y en algunos países incluso experimentales, puede resultar complicado para las instituciones financieras promotoras de dichos servicios encontrar una proporcionalidad en su nuevo rol de supervisor, puesto que aún no hay guías o estándares. Esto puede derivar en la imposición de excesivos controles tanto en las fases de integración como de posterior seguimiento de los negocios, ahogando a las *FinTech* consumidoras de los servicios, o, en el otro extremo, pecar de falta de filtrado inicial o seguimiento parcial, no controlando o careciendo de una visión global de los riesgos que suponen este nuevo tipo de servicios. Por este motivo, las instituciones financieras han de plantearse previo a la oferta de este tipo de servicios si están técnica y culturalmente preparadas para este tipo de negocios, dado que implica requerimientos de mayor flexibilidad, reducción de tiempos de respuesta y aumento del apetito de riesgo<sup>78</sup> de las organizaciones.

El ofrecimiento de este tipo de servicios por entidades tradicionales puede implicar esfuerzos no solo de carácter tecnológico, sino también cambios más profundos en elementos base de la propia organización. Las *FinTech* son entidades con alto componente tecnológico, por lo que la gestión del propio proyecto requiere que las personas involucradas no solo cuenten con los clásicos conocimientos de negocios financieros, sino que también comprendan los requerimientos e implicaciones tecnológicas, organizativas y de control. Esto se extiende a los propios contratos y acuerdos de niveles de servicios, que cuentan con una carga alta de conceptos técnicos que los equipos legales deben revisar. Por esta razón, las instituciones financieras tradicionales deben plantearse si cuentan con personal con los niveles de especialización y conocimientos que se requieren para estos nuevos modelos ya no enfocados en los negocios, sino en la tecnología, para que puedan ser capaces de asesorar a la entidad adecuadamente.

---

<sup>78</sup> Se refiere al “nivel agregado y tipos de riesgo que una institución financiera está dispuesta a aceptar, o evitar, con el fin de lograr sus objetivos comerciales” (Financial Stability Board [FSB], 2013, p. 3).

Las entidades que ofrezcan este servicio deberán considerar qué estrategia de gestión del cambio emplean en la oferta de servicios, teniendo en cuenta que cada módulo puede implicar un nivel distinto de esfuerzo de implementación, complejidad de arquitectura y rentabilidad. Por ejemplo, las API de acceso y autenticación no son complejas; sin embargo, los módulos relacionados con pagos internacionales conllevan un nivel más alto de esfuerzo y complejidad, a cambio de una mayor rentabilidad (Cognizant, 2016, pp. 1-20).

### 5.8.3 Derivadas post-contractuales: diligencia debida

Al igual que los modelos de delegación de funciones críticas en banca, la entidad promotora de las iniciativas de BaaS o FaaS deberá asesorar el nivel de riesgo de la contraparte que será su comisionista o agente, con el fin de diseñar modelos de diligencia debida y gestión de riesgos proporcionales a la exposición que representen. Las funciones que el agente llegue a realizar presentarán enfoques en temáticas diferentes (por ejemplo, *FinTech* a las que se cedan elementos relacionados con *software* sin compartir datos personales de cliente tendrán controles distintos a aquellas *FinTech* a las que se les hace agentes de captación y obtención de datos relacionados con elementos de prevención de lavado de activos y financiación del terrorismo).

Por lo anterior, la documentación de inducción de las *FinTech* en estos casos deberá adaptarse a los servicios delegados. Del mismo modo, siguiendo un enfoque basado en riesgos, el nivel de exigencia de información en el seguimiento de las actividades de la *FinTech* (en términos de profundidad y frecuencia) dependerá de las actividades que la *FinTech* desarrolle para las entidades financieras o *FinTech* licenciadas. A lo largo del ciclo de vida de la relación entre las partes, estos controles habrán de adaptarse a los cambios en los servicios delegados.

### 5.8.4 Desde el punto de vista de los consumidores y usuarios

Otra área gris que plantean estos modelos es la transparencia de este encaje de bolillos de cara a los clientes y cómo explicar esta complejidad de una forma llana y sencilla. El cliente ha de ser consciente de la entidad con la que contrata los servicios financieros regulados y de la entidad que funciona como captador o frontal tecnológico. Si bien es cierto que este hecho se hace obvio en el momento de la aceptación de los contratos (por lo general, el usuario verá que acepta unos términos y condiciones de uso de plataforma



no regulada, documentos relativos a las protección de datos y cesión de datos de la plataforma no regulada, y los contratos pertenecientes a la entidad financiera o *FinTech* con licencia, junto con sus documentos relativos a protección de datos), lo habitual será mostrar logos de ambas entidades en las pantallas compartidas o el desarrollo de *banner*, *pop ups* o herramientas similares que permitan al usuario conocer estas circunstancias.

En línea con lo anterior y en relación con la fragmentación de las cadenas de valor, se argumenta la cuestión de quién se encarga de qué en caso de que haya incidencias. Si bien es cierto que el primer filtrado de incidencias está en la entidad consumidora del servicio BaaS o FaaS, sus equipos de atención al cliente deben formarse para tener conocimiento de las respuestas modelo que espera la entidad que cede la licencia, con el fin de estandarizar los procesos. En ocasiones, el incluir un filtrado más puede implicar un mayor tiempo de respuesta o de resolución de conflictos, añadiendo complejidad a los procesos y corriendo el riesgo de que los usuarios se sientan no atendidos (la percepción temporal en servicios financieros móviles es más corta que la presencial). En problemáticas como esta, los acuerdos de niveles de servicio juegan un papel clave en la relación entre las partes.

### ***5.9 Propuesta de criterios mínimos legales y regulatorias***

Como ya se ha explicado a lo largo de este documento, la posición de esta tesis es que no existe un único modelo de BaaS y FaaS. En efecto, al tratarse de iniciativas privadas innovadoras, que aún no son materia de regulación, se presentan diversas variables y no existen criterios ni estándares uniformes. Lo cierto es que, en todos los casos, BaaS y FaaS son modelos empleados con mayor auge en países en los que se promueven esquemas de banca abierta y por parte de entidades financieras que están más avanzadas en su transformación digital.

La diversidad en modelos y en enfoques supervisores obstaculiza la masificación del modelo de BaaS y FaaS. Sin duda, en un mundo financiero global y dinámico, las innovaciones que aportan valor como estas requieren estándares uniformes o criterios mínimos, de modo que puedan ser masivamente adoptadas. Por tanto, en aras de lograr un consenso que permita masificar el BaaS y el FaaS, los siguientes criterios mínimos deberían considerarse en toda regulación:

Primero, el enfoque de los reguladores debería basarse en riesgos y plantearse bajo un criterio de proporcionalidad. Ello quiere decir que, a mayor riesgo en el modelo de BaaS

y FaaS, más estrictos deberán ser los controles. En efecto, no es lo mismo proveer un módulo de servicios bancarios bajo estos modelos (por ejemplo, pagos) que un servicio integral bajo el concepto de “llave en mano”. En casos de servicios menores, la opción de notificación podría ser factible, mientras que en los esquemas integrales podría hacerse necesario un proceso de autorización previa, siempre y cuando los tiempos no sean gravosos (por ejemplo, evaluación por parte de las autoridades en el plazo de uno a tres meses desde la entrega de la documentación).

Segundo, los reguladores deberían evaluar, cuando menos, los siguientes riesgos que están presentes en todo esquema de banca abierta y, concretamente, en las variantes de BaaS y FaaS. Tales riesgos son los que afectan los datos personales, la seguridad de la información y ciberseguridad, la protección al usuario y la integridad de los mercados (lavado de activos y corrupción).

Cualquiera que sea la opción regulatoria, no debe perderse de vista que la licencia financiera es el permiso gubernamental que se otorga a una entidad para prestar al público los servicios financieros regulados bajo la supervisión de la autoridad, asumiendo dicha entidad la entera responsabilidad por los servicios que presta, tanto frente al público como frente a las autoridades. Si una entidad financiera decide operar bajo el modelo BaaS, debe ser consciente de que continuará asumiendo la responsabilidad por los servicios que brinda al público, así lo haga bajo una marca compartida, con un proveedor tecnológico o con cualquier empresa con la que decida tercerizar parte de sus procesos de servicios. Dicha responsabilidad puede ser administrativa, civil o incluso penal.

Lo anterior supondrá para la entidad financiera que deba elegir bien a su contraparte, efectuando una debida diligencia previa; y asegurarse de que con ella tendrá niveles de servicios (SLA) que le permitan gestionar adecuadamente cuando menos los riesgos indicados. La relación contractual entre entidad financiera y empresa no regulada se tornará fundamental para asegurar una adecuada gestión de los riesgos asociados al BaaS y FaaS. En ese sentido, el rol de las autoridades en este ámbito debería limitarse a fijar los criterios mínimos de dicha gestión de riesgos y a supervisar, de manera posterior (supervisión *ex post*), que estos estén siendo adecuadamente manejados. No es recomendable que el supervisor autorice de manera previa este tipo de contratos ni mucho menos que establezca *a priori* la figura jurídica que deberán emplear las partes para hacer viable el BaaS o FaaS. Ello podría obstaculizar el desarrollo de este modelo, puesto que,

como se explicó, no existe una forma única de hacerlo y el objetivo es que se masifique, por lo cual la regulación debería ser flexible.

En cualquier escenario, deberán cuidarse las implicaciones regulatorias una vez concluido el BaaS o FaaS. En efecto, cualquiera que sea la estructura jurídica elegida para implementar el BaaS y el FaaS, deberá considerarse el carácter temporal de este servicio, dado que, en la mayoría de los casos, lo que la empresa no regulada quiere es obtener su propia licencia. En tal sentido, dicha estructura jurídica debería prever cuestiones mínimas respecto a la transición y cierre ordenado una vez que la *FinTech* obtenga su propia licencia.

#### **IV. FINTECH 3.0 y 3.5: ¿DESINTERMEDIACIÓN O REINTERMEDIACIÓN?**

Tras haber analizado la transformación de la industria financiera, cabe concluir que, efectivamente, se está experimentando una reducción de la concentración de la oferta de servicios financieros en un solo proveedor o en la banca tradicional, a favor de una mayor especialización o de estrategias de nicho. Por tanto, se produce un fraccionamiento de la cadena de valor y la entrada de nuevos agentes identificables, hablando así de una descentralización centralizada o CeDeFi.

Estas actividades abren una nueva problemática para los reguladores y supervisores, puesto que la normativa existente ya no es del todo adecuada debido a que no captura ni las nuevas contrapartes con origen tecnológico, ni son capaces de ver la granularidad que han alcanzado estas fragmentaciones de las cadenas de valor de los servicios financieros (ejemplo de BaaS o FaaS). Ello se agrava en aquellos casos en los que la normativa está basada en entidades y no en actividades, dado que requiere de modificaciones para poder extender su ámbito a estas nuevas contrapartes, tal y como sucedió en la PSD II con los terceros proveedores de servicios de pagos. Además, surgen problemas globales en los que no queda clara la jurisdicción encargada o el supervisor a cargo.

Por otro lado, las industrias de origen de estos actores son híbridas como mínimo, lo que hace difícil conocer el límite supervisor e incluso conocer el riesgo a nivel global (casos de los *Marketplace* que vuelven a concentrar servicios, pero de una forma diferente y de industrias distintas). Por ello, se defiende que de hecho se produce un nuevo fenómeno que consiste en desdibujar los límites entre las industrias, especialmente las tecnológicas y de comunicaciones.

Esta nueva unión o asociación de negocios puede identificarse como una reintermediación de actividades reguladas y no reguladas o que se encuentran bajo supervisión de distintas autoridades. Por tal razón, surge la pregunta de si será necesario una solución de supervisión híbrida en un futuro o un régimen regulatorio en ese sentido, especialmente en lo que respecta a los gigantes tecnológicos con la finalidad de poder asesorar el riesgo del modelo de negocio de una manera integral y así poder captar dinámicas que de otro modo podrían no ser capturadas por las autoridades al quedarse en tierra de nadie.

En suma, los supervisores tendrán que establecer, al menos, criterios de colaboración o comités de supervisión (ya sea intersectorial o supranacional) que permitan un adecuado asesoramiento de los riesgos de reintermediación. Todos estos elementos abordados a lo largo de este capítulo permiten concluir que *FinTech* 3.0-3.5 ya no son etapas evolutivas, sino de disrupción.

## **V. RECAPITULACIÓN. ANÁLISIS DE MARCOS REGULATORIOS Y DE SUPERVISIÓN *FINTECH* 3.5**

Frente al reto de regular el universo de actividades *FinTech* antes indicadas, y la pregunta de si hacerlas encajar en contextos existentes o desarrollar normativa *ad hoc*, la UE parece haber tomado un enfoque mixto.

En ciertos casos, como es el de las actividades de plataformas de financiación participativa o la emisión de dinero electrónico, se ha optado por llevar a cabo desarrollos normativos *ad hoc* o *ex novo* debido a la materialidad y a la diferencia sustancial con respecto a las regulaciones ya existentes. También se ha observado la generación de regulación no financiera con el fin de hacer frente a la aparición de entidades con impacto generalizado en servicios financieros y no financieros. Este es el supuesto de las *BigTech* que ofrecen servicios a través de plataformas digitales y que en la actualidad se regulan en la UE mediante el DMA y el DSA que se tratarán en la segunda parte de esta tesis.

En otros casos, se ha optado por interpretar la inclusión de estos modelos de forma total o parcial en los esquemas normativos existentes (principalmente PSD II o MiFID II), ya sea mediante actualizaciones de la regulación existente para dar cabida a los nuevos participantes y modelos (PSD II con los iniciadores de servicios de pago y los agregadores) o mediante interpretaciones extensivas (por analogía) de la regulación existente. Sin embargo, estas interpretaciones parecen ser soluciones temporales o

parciales hasta que se especifique cómo tratar estas actividades en profundidad. Un ejemplo de ello son los *robo advisors* o el *social trading*, a los que se les ha venido a aplicar una extensión por analogía del ámbito de MiFID II.

En ese sentido, no se puede dejar de observar que existen actividades que parecen caer fuera de los perímetros regulatorios actuales o que han podido considerarse de prioridad o materialidad menor a la hora de valorar posibles esfuerzos de producción normativa, siguiendo el principio de las lagunas normativas, por el que aquellas realidades no reguladas se consideran no relevantes desde la perspectiva jurídica.

En consecuencia, cabe concluir que las finanzas abiertas en la UE, a diferencia de América Latina, no han contado con una regulación marco *ad hoc*, sino que se ha tomado un enfoque que podría categorizarse como de basado en riesgos, por el que se ha priorizado la producción de normas de modelos y contrapartes sustancialmente distintos, seguido de la revisión y actualización de contextos normativos existentes. En último lugar, se han llevado a cabo interpretaciones extensivas por analogía de ciertas normativas para acoger nuevas actividades o incluso se ha llegado a no regular ciertas actividades propias de las finanzas abiertas.

Las principales piezas regulatorias propias de esta etapa en Europa están relacionadas con la emisión de dinero electrónico y las plataformas de financiación participativa, siguiendo el esquema de la pirámide de necesidades financieras que se presentó previamente. Sin embargo, otras actividades como la inversión o los seguros parecen haber carecido de prioridad suficiente para generar sus propios desarrollos normativos. Además, parecen haberse postergado aún más a raíz de la preponderancia que ha tomado la etapa *FinTech 4.0* que se verá en el capítulo siguiente, y que han llevado a la necesidad de grandes piezas regulatorias propias, como es la propuesta del MiCA.

Asimismo, los entornos de supervisión han seguido la estela de la regulación, focalizándose en aquellos modelos de negocio que presentaban mayor materialidad y novedad. No obstante, siguiendo este enfoque basado en riesgos y, debido a que la gran mayoría de las entidades *FinTech* no han estado reguladas, tan solo aquellas que formalmente han pedido una licencia, ya sea bancaria o más ligera, han estado sujetas a supervisión.

En efecto, el propio regulador ha acogido la innovación para ser capaz de llevar a cabo supervisiones en tiempo real, adaptándose a la inmediatez con la que está operando la

industria hoy en día. Ello se ha conseguido mediante modelos de tecnología en supervisión o *SupTech*. Se puede identificar un mayor foco o extensión supervisora en determinados aspectos, que suelen estar relacionados con protección a consumidores y con crimen financiero. A este respecto, las directivas de prevención de blanqueo han ido aumentando su ámbito de sujetos obligados a través de la quinta y sexta directivas, requiriendo que muchas *FinTech* se sometan a un registro de sujetos obligados. De esa manera, entran dentro de perímetros de control como entidades registradas en términos de prevención de blanqueo de capitales y prevención de financiación del terrorismo.

Finalmente, se vuelve a tomar un enfoque selectivo basado en riesgos incluso en las materias, puesto que crimen financiero se considera una prioridad, debido a que existe tolerancia baja hacia este tipo de incumplimientos.

## CAPÍTULO IV. *FINTECH* 4.0: LA DISRUPCIÓN

### I. INTRODUCCIÓN: CONTEXTO GENERAL

Las DeFi surgieron como una radicalización de los principios de finanzas abiertas. Si bien las finanzas abiertas abocan por devolver la hegemonía y capacidad de decisión de los datos financieros a sus usuarios para que puedan tomar mejores decisiones, estas siguen basadas en principios de centralización, es decir, un ente regulador, un ente emisor y personas jurídicas que ofrecen el servicio. En definitiva, terceros de confianza.

Sin embargo, las DeFi van un paso más allá en este concepto, combinando las finanzas abiertas con ideas del denominado movimiento de los *cyberpunks* (Caballero et al., 2020, p. 75), que considera que parte del problema de las crisis financieras son los monopolios del dinero por parte de los bancos e instituciones centralizadas. Por este motivo, las DeFi se proyectan como un tipo de espacio financiero en el que se busca evitar esa figura del tercero de confianza, mediante el uso de soluciones tecnológicas. Esta descentralización incluye no solo los servicios financieros, sino también las propias monedas o activos, dando paso a los denominados criptoactivos que han tenido una rápida acogida.

La adopción cripto institucional pasó del 45 % en 2020 al 56 % en 2022, y la individual es una media del 10 % en los principales países de la UE, con una inversión media de entre 1000 y 5000 euros (European Central Bank [ECB], 2022a, pp. 1-20). En España, el perfil del usuario cripto ronda entre los 25 a 44 años, siendo principalmente hombres (66 %) con estudios universitarios (43 %) (Comisión Nacional del Mercado de Valores [CNMV], 2022, pp. 1-39).

Pese al crecimiento del fenómeno de las DeFi y los criptoactivos a lo largo de los últimos años y su potencial de disrupción en los años por venir, aún existe escasa literatura académica que proponga soluciones flexibles para la reducción de los riesgos de tipo regulatorio y de supervisión, con el fin de que esta nueva forma de hacer finanzas adquiriera un mayor nivel de seguridad jurídica y, por tanto, aceptación de distintos estamentos de la sociedad.

En el presente capítulo, se formulan primeramente las bases tecnológicas que han dado pie al surgimiento de los criptoactivos y las DeFi, realizando un acercamiento hacia el nuevo tipo de esquemas de organización y gobernanza. Posteriormente, se aborda el

concepto de DeFi, su propósito, diferencias con las finanzas tradicionales o centralizadas, sus contrapartes e infraestructura. Seguidamente, se exponen las variedades de criptomonedas que podrán operar en las DeFi y los cambios que estas generan en las actividades que llevan a cabo de pasivo, activo, inversión y otro tipo de servicios, así como el rol de la banca institucional en esta nueva era.

Tras haber delimitado el universo de actividades DeFi, se realiza un análisis del marco regulatorio actual en la UE, con el fin de desarrollar las problemáticas que se plantean tanto desde el punto de vista desde el de supervisión. Finalmente, se expone cómo estos elementos (criptoactivos y DeFi) se engranan dentro de un soporte aún más innovador, esto es, el metaverso.

El presente trabajo se desarrolla desde una metodología teleológica, puesto que busca evaluar qué elementos normativos son requeridos para que las DeFi puedan ser efectivas herramientas operativas. Para ello, se lleva a cabo una revisión de literatura, normativa, guías de organismos globales, así como un análisis de los libros blancos desarrollados por los propios protocolos y plataformas DeFi.

La hipótesis de la que se parte es que, pese a que las DeFi tienen gran potencial, en la actualidad no cuentan con los entornos de seguridad jurídica y de control suficientes para considerarse una solución de aplicación inmediata. Este capítulo busca analizar y delinear el universo de las DeFi, su utilidad como actividades financieras de los Metaversos, y proponer la necesidad de que las políticas regulatorias sigan un enfoque basado en riesgos y sean proporcionales.

## **II. ELEMENTOS DE CARACTERIZACIÓN**

### **1. *Blockchain* como puerta de acceso**

Las DeFi han sido posibles gracias a la DLT, que son bases de datos no centralizadas, gestionadas por distintos participantes sin que exista una única figura de verificador. Por tal razón, se consideró importante abordar elementos básicos de *Blockchain* para poder comprender posteriormente el entorno de las DeFi.

*Blockchain* o cadena de bloques es un tipo específico de DLT que forma bloques, unidos unos a otros a través de claves criptográficas (*hash*) como forma de comprobación de que la información no es manipulada. Puede definirse como “un libro de registro inmutable que contiene la historia completa de todas las transacciones que se han



ejecutado en la red, a cada participante se le llama nodo, que en realidad viene a ser un ordenador más o menos potente” (Ortega, 2019, p. 24). También pueden definirse de la siguiente manera:

*Fundamentalmente protocolos de software que permiten que múltiples partes operen bajo suposiciones y datos compartidos sin confiar entre sí. Estos datos pueden ser cualquier cosa, como información de ubicación y destino de elementos en una cadena de suministro o saldos de cuentas de un token. Las actualizaciones se empaquetan en “bloques” y se “encadenan” entre sí criptográficamente para permitir una auditoría del historial anterior, de ahí el nombre.* (Campbell et al., 2021, p. 13)

Los protocolos son conjuntos de criterios o reglas que permiten la transmisión de datos e información entre dos o más máquinas (Pérez, 2019, pp. 141-177). Existen distintos tipos de *Blockchain*, dependiendo del grado de apertura al público (esto es, la capacidad de establecer un nodo, participar en toma de decisiones o crear en base a la cadena de bloques): (i) cadenas privadas de acceso a determinadas contrapartes previa autorización del administrador del sistema, por lo que los participantes en esta están identificados (Jensen et al., 2021, p. 47); (ii) de consorcio, que requiere permiso de acceso para miembros de un colectivo; y (iii) públicas, en las que cualquier persona puede participar de distintas formas, sin permiso previo (Ortega, 2019, pp. 27-27).

Como puede verse, esta tecnología cuenta con un potencial de aplicación no solo en la industria financiera, sino también en un rango de actividades mucho mayor. En concreto, *Blockchain* puede aplicarse en ciertos elementos de mejora de los sistemas y operativas de las finanzas tradicionales tal y como se les conoce hoy en día, por ejemplo, en identidad digital para conocimiento de clientes (Pascual, 2017, pp. 1-5), emisión de bonos (European Investment Bank [EIB], 2021, pp. 1-3), operaciones de importación y exportación (Deloitte, s.f., pp. 1-2), o incluso mejora de los sistemas de compensación y liquidación en infraestructuras financieras (Priem, 2020, pp. 1-25).

Sin embargo, ha sido reconocida por el público en general debido a que es la tecnología aplicada las finanzas del futuro, esto es, criptoactivos como *bitcoin*<sup>79</sup> (Nakamoto, 2008,

---

<sup>79</sup> “*Bitcoin*” (con mayúscula) se emplea para hacer referencia a la cadena de bloques, mientras que “*bitcoin*” con minúscula se refiere a la criptomoneda. Este criterio (mayúscula para la cadena de bloques, minúscula para el criptoactivo) se replica en todos aquellos casos en los que el *token* nativo y la *Blockchain* coinciden en nombre.

pp. 1-9) o infraestructuras de DeFi como Ethereum (Ethereum, 2021a, pp. 1-36). Tanto *Blockchain* como su moneda estandarte *bitcoin* combinan elementos que no eran novedosos en sí (ver Tabla 8). A modo de ejemplo, el concepto criptográfico de *hash* indicado anteriormente ya se consideraba en 1990 (Haber y Stornetta, 1990, pp. 437-455). Es la combinación de estos conceptos, las mejoras en la potencia computacional y la crisis financiera, lo que impulsa estos nuevos modelos auspiciados una filosofía subyacente<sup>80</sup>. Este movimiento se caracteriza por estar en contra del control gubernamental y de los bancos centrales, y en pro de las finanzas lideradas por la tecnológica y no por los países (Caballero, 2019, p. 45).

A continuación, en la Tabla 8 se exponen los principales conceptos que se aglutinan en las DeFi, junto con las obras que dieron origen a estas ideas, sus autores y el año. Como se puede observar, numerosos elementos no son ni mucho menos novedosos, pero es la combinación de estos en una solución tecnológica lo que brinda la novedad.

<b>Concepto</b>	<b>Origen</b>	<b>Autor</b>	<b>Año</b>
Crecimiento exponencial de la capacidad de procesamiento de datos.	<i>Cramming more components onto integrated circuits</i>	Moore, G. E.	1965
Pagos digitales aplicando criptografía.	<i>Blind signatures for untraceable payments</i>	Chaum, D.	1983
No trazabilidad a la vez que se evita el doble gasto en transacciones similares al efectivo.	<i>Untraceable electronic cash</i>	Chaum, D., Fiat, A., & Naor, M.	1988
Hash y prueba de trabajo ( <i>proof of work</i> o PoW).	<i>How to time-stamp a digital document</i>	Haber, S., & Stornetta, W.	1990
Anonimato en pagos aplicando criptografía.	<i>Zero-knowledge undeniable signatures</i>	Chaum, D.	1990
Aumentar nivel de dificultad computacional en casos de envíos masivos de <i>mails</i> .	<i>Pricing via processing or combatting junk mail</i>	Dwork, C., & Naor, M.	1992
Contratos inteligentes.	<i>Can computers make contracts?</i>	Allen, T., y Widdison, R.	1996
Contratos inteligentes.	<i>Formalizing and securing relationships on public networks</i>	Szabo, N.	1997

<sup>80</sup> El pensamiento subyacente consiste en evitar el control de instituciones financieras tradicionales (agentes financieros, bancos centrales, autoridades), puesto que estos generaron o no pudieron evitar las crisis financieras anteriores y, por ello, se ha de desconfiar.

Dinero semidescentralizado y anónimo	<i>B-money</i>	Dai, W.	1998
<i>Hash.</i>	<i>Hashcash-a denial of service counter-measure</i>	Back A.	2002

Tabla 8. Origen de conceptos aplicados en Blockchain y Bitcoin

Nota. Elaboración propia, adaptado de *Bitcoin. Blockchain y tokenización para inquietos*, por M.Caballero, Bubock Editorial.

Debido a la filosofía que respalda estas iniciativas, el diseño tecnológico cuenta con ciertos elementos característicos:

El primer componente es la privacidad, obtenida mediante el empleo de la criptografía asimétrica (Pascual, 2017, pp. 1-5). Esto significa que los participantes en las operaciones cuentan con dos claves: una pública y una privada (semejante a una contraseña de cada participante). La dirección pública se define como “un código numérico largo que se deriva criptográficamente de una clave privada específica. (...) La clave pública debe emparejarse con la clave privada correspondiente correcta para que se ejecute una transacción” (Deloitte y Dubai Financial Services Authority, 2022, p. 5).

La clave privada consiste en “un número binario generado aleatoriamente que se usa para cifrar y descifrar información, y es solo puesto a disposición del autor del contenido cifrado. Posteriormente, esta clave privada es todo lo que se requiere para confirmar una transacción” (Deloitte y Dubai Financial Services Authority, 2022, p. 5). En la Figura 27 puede verse un ejemplo de cómo funciona la operativa. Primeramente, un usuario “A” envía su clave pública al usuario “B”. Una vez recibida, el usuario “B” puede encriptar y autorizar la transacción. Finalmente, el usuario “A” usa la clave privada para descifrar y aceptar la transacción.

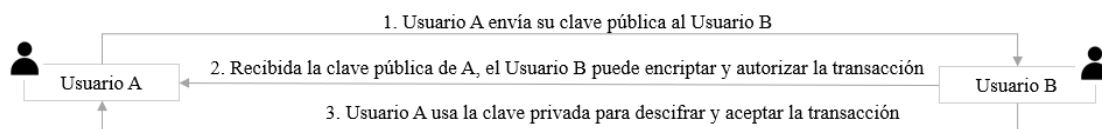


Figura 27 Operativa con claves criptográficas públicas y privadas

Nota. Tomado de *A Market Overview of Custody for Digital Assets. Digital Custodian Whitepaper*, Deloitte y Dubai Financial Services Authority, 2022, p. 5, Deloitte.

Asimismo, la inmutabilidad y descentralización son ingredientes propios de las cadenas de bloques, y son provistas mediante la tecnología *Blockchain* y las funciones de

los nodos<sup>81</sup>. Finalmente, se conciben como un mecanismo de consenso para poder dar el bloque por válido y, por tanto, añadirse a la cadena de forma legítima. A este respecto, existen distintos tipos de mecanismo de consenso<sup>82</sup>.

Los mecanismos de consenso más conocidos son la prueba de trabajo (*proof of work* o PoW), la prueba de participación (*proof of stake* o PoS) y la prueba de participación delegada (*delegated proof of stake* o DPoS). Existen también mecanismos de consenso menos utilizados, como la prueba de la velocidad (*proof of stake velocity* o PoSV), la prueba de autoridad (*proof of authority* o PoA) y la prueba de quemado (*proof of burn* o PoB) (Guaita et al., 2019, pp. 5-160). A continuación, se explican brevemente los dos mecanismos de consenso más habituales:

La PoW es un tipo de algoritmo de consenso por el que los participantes (denominados mineros) compiten por validar transacciones. Para ello, se requiere que sus equipos informáticos sean capaces de resolver problemas matemáticos que reclaman cierto esfuerzo computacional. El primero que resuelve el problema, valida la operación y genera un nuevo bloque en la DLT. Este tipo de consenso es el empleado por *Bitcoin*.

La PoS surgió debido a que los algoritmos de prueba de consenso consumen tiempo y esfuerzo computacional. De esa manera, el PoS da peso a elementos tales como el tiempo que el equipo informático lleve participando en la red o la cantidad de criptoactivos propios de la cadena o protocolo que se posean. Entre ellos, se realizará una selección aleatoria de nodos que serán los que validen la transacción. Ethereum es un ejemplo de uso de este tipo de consenso. En su caso, esta *Blockchain* pasó del uso de la prueba de trabajo a la prueba de participación en 2022 con la denominada Ethereum 2.0 (Ethereum, 2021b, pp. 1-5).

## **2. Los contratos inteligentes como nuevo sistema de establecimiento de reglas**

Los contratos inteligentes o *smart contracts* pueden definirse como un “código de *software* basado en *Blockchain* que realiza, controla y documenta eventos y acciones relevantes de acuerdo con términos y reglas predefinidos” (Wharton School, Digital Asset Project, World Economic Forum, 2020, p. 1-20). Asimismo, son:

---

<sup>81</sup> Se denominan nodos a las computadoras que, conectadas entre sí a la *Blockchain*, ejecutan el *software* necesario para su operativa. Esta figura se desarrolla más adelante.

<sup>82</sup> El mecanismo de consenso es la forma de dar la validación de la integridad de la cadena de bloques.

*Secuencias de instrucciones o indicaciones que serán utilizadas, de forma directa o indirecta, en un sistema informático, con el objetivo de realizar algunas prestaciones de un contrato, con la particularidad de que, una vez activadas, las partes dejan de tener el control de su cumplimiento, ya que se realizará por sí mismo.* (Ortega, 2019, p. 1)

El término se asocia a Nick Szabo, quien en 1994 propuso que los códigos informáticos se emplearan de forma similar a la de una máquina expendedora en la que, si se mete dinero, se obtiene un refresco. Es decir, si se da una condición “A”, entonces sucede una consecuencia “B” (Barrio, 2020, pp. 80-87).

Los contratos inteligentes se caracterizan por operar dentro de una *Blockchain*, eliminando la necesidad de un tercero de confianza para el procesamiento de operaciones (societarias o financieras) y contando con la característica de ser inalterable una vez se ejecuta. Además, gozan de la capacidad de llevar a cabo una acción automática si se cumplen las condiciones o eventos que se hayan indicado en su código. Estas condiciones pueden ser simples o pueden requerir de la captura de información del exterior. En esos casos, los contratos inteligentes obtienen información de los denominados oráculos, los cuales se analizan más adelante.

En general, los *smart contracts* se basan en lógicas por las que, si se da un supuesto, en consecuencia, se produce un efecto (si-entonces). Por ello, la autora coincide con la postura de Martinero Tor, por lo que no pueden catalogarse como contratos completos conforme a los principios del Código Civil (CC), puesto que no llegan a cumplir las estructuras de consentimiento, objeto y causa que le otorguen plena validez (Martinero, 2022, p. 332).

Los *smart contract* pueden cubrir distintos tipos de actividades dentro del mundo de las nuevas DeFi:

Desde el punto de vista equiparable de derecho societario, los contratos inteligentes pueden operar de manera similar a una escritura de constitución y acuerdos sociales, incluyendo modificación de estatutos u órganos de gobierno de organizaciones autónomas descentralizadas (*decentralized autonomous organizations* o DAO). De esta forma, el contenido de los contratos inteligentes se vuelve la ley, por lo que cabe la posibilidad de operar sin necesidad de establecer una entidad con personalidad jurídica propia acorde con la regulación local de un país. En ese sentido, tomando el código informático como base de toma de decisiones, no se requiere de personas o estructuras de

tipo centralizado. Este tipo de usos se puso en marcha en Alemania en el año 2016, pero el proyecto tuvo que ser abandonado debido a un robo informático de parte de los fondos aportados (Barrio, 2020, p. 84). Las DAO se analizan detalladamente dentro de este capítulo.

Por otro lado, los contratos inteligentes también se emplean de forma análoga a los contratos legales en el mundo tecnológico, pero aplicando lenguaje y terminología de programación global, en sustitución de la jerga legal específica de la jurisdicción. De nuevo, por lo general, el código reemplaza a los tradicionales formatos de acuerdos legales entre las partes. Pese a ello, los *smart contracts* no reemplazan todas las cláusulas legales existentes habitualmente (por ejemplo, ley aplicable y jurisdicción competente, derechos y obligaciones de las partes o clausulados propios de transparencia, conflictos de interés y protección al consumidor).

Finalmente, este tipo de códigos también es la base para la creación de *tokens*, entre ellos los criptoactivos, incluyendo las criptomonedas; sin embargo, tal y como se verá en el análisis crítico de la iniciativa europea de MiCA<sup>83</sup> (*Markets in Crypto Assets*), los contratos inteligentes de carácter financiero no se encuentran regulados en la actualidad, pese a que son la base de todas las finanzas y criptoactivos que operan bajo *Blockchain*. En ese sentido, el “dinero programable” o las operaciones sujetas a condiciones incrustadas en el contrato inteligente carecen de procesos de control o verificación (por ejemplo, asegurarse que el lenguaje no sea texto plano sino ejecutable). Es decir, uno de los componentes más novedosos de esta tecnología, como el dinero programable, se mantienen inexplorados en las principales piezas regulatorias de la UE, cuando, a este respecto, sería altamente recomendable establecer ciertos criterios de mínimos, tales como programar que los criptoactivos no puedan enviarse a direcciones de billeteras sancionadas.

Los *smart contract*, como nuevo sistema de establecimiento de reglas, abren varios riesgos que deben considerarse. El primero de ellos es cuestionarse si estos programas pueden reemplazar realmente un contrato o no. La posición de la autora es que hoy por hoy, debido a la falta de adaptación de los ordenamientos jurídicos, los contratos

---

<sup>83</sup> Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937.

inteligentes no pueden reemplazar totalmente las estructuras contractuales existentes, requiriendo, por tanto, una duplicidad en el aspecto legal (parcial o total).

Además, se genera una segunda cuestión, que es clave y se repite en todos los proyectos de DeFi: la falta de claridad respecto a los criterios para fijar qué jurisdicción y tribunales aplica, máxime cuando las partes se encuentran dispersas en distintas jurisdicciones. La cuestión se hace aún más retadora si se tiene en cuenta que en muchos de estos *smart contract* las partes son máquinas (es decir, ya no se habla de contratos de consumidor a negocio o negocio a negocio, sino de contratos máquina a máquina o M2M) (Barrio, 2020, p. 86).

En relación con los dos problemas anteriores, surge la duda de los regímenes de obligaciones de las partes involucradas, no siendo claro y generando riesgos de vacíos de responsabilidad. Este elemento se hace esencial, máxime cuando los *smart contracts* generan almacenamientos masivos de datos de todo tipo y están expuestos a riesgo de *hackeos* debido a la generación de códigos incompletos o deficientes (Barrio, 2020, p. 86). Estos riesgos deben controlarse, dado que los *smart contracts* son la base para el desarrollo de los *token*, las DAO y las DeFi, como se aborda a continuación.

### **3. Los *tokens* o fichas**

Los *tokens* o fichas se definen como una combinación de caracteres alfanuméricos que, dependiendo de su diseño, pueden representar distintos tipos activos o derechos en las cadenas de registros distribuidos o en los diferentes protocolos que operan sobre cadenas de registros distribuidos. Los *tokens* no son exclusivos del mundo *Blockchain* o de las DeFi, sino que son un concepto que puede emplearse en el nivel de la DLT. Los *tokens* adoptados en el mundo de las DeFi, comúnmente conocidos como criptomonedas o criptodivisas, serán objeto de análisis posterior.

La taxonomía o clasificación de las fichas tiene, por tanto, un carácter poliédrico que atiende a diversos planos que deben verse en su conjunto, comenzando por la industria, la finalidad, la tecnología que aplica, la forma de distribución, los derechos que otorga o los mecanismos de consenso que aplican al *token*. En la actualidad, ya han surgido iniciativas de estandarización y clasificación de *tokens*, como la desarrollada por la International Token Standarization Association (ITSA) (ITSA, 2019, pp. 1-12).

La Tabla 9 muestra una combinación de ejemplos de posibles dimensiones que se podrían tener en cuenta de cara a la realización de taxonomías de *tokens* (por ejemplo, la

industria que los emplearía, el público objetivo, el uso, los derechos que otorga, la tecnología, el mecanismo de consenso o de distribución).

<b>Dimensión</b>	<b>Concepto</b>	<b>Ejemplos</b>
Industria	Industria en la que se usa el <i>token</i> .	Finanzas, arte, entretenimiento.
Público	Destinatarios del <i>token</i> .	Minorista o mayorista.
Uso	Propósito económico.	Medio de pago, inversión, gobernanza (capacidad de voto y decisión sobre productos y protocolo), mecanismo de compensación y liquidación ( <i>settlement token</i> ).
Derechos	Derechos que otorga.	No da derechos, derechos limitados, derechos absolutos.
Tecnología	Capa sobre la que se diseña.	La propia DLT o protocolo sobre esta.
Consenso	Mecanismo de consenso o gobernanza.	Prueba de trabajo, prueba de participación, prueba de participación delegada.
Distribución	Mecanismo de distribución del <i>token</i> .	Oferta inicial de monedas (ICO), acuerdo de futuros <i>tokens</i> (SAFT), asignación interna, asignación automática a participantes activos, asignación automática a participantes pasivos.

Tabla 9. Ejemplo de dimensiones para tener en cuenta para catalogar un token

Nota. Elaboración propia, adaptado de *Setting standards for global token markets*, International Token Standardization Association, 2019, [https://www.bvi.de/fileadmin/user\\_upload/Regulierung/Branchenstandards/20190125\\_-\\_ITSA\\_-\\_Setting\\_Standards\\_for\\_Global-Token-Markets.pdf](https://www.bvi.de/fileadmin/user_upload/Regulierung/Branchenstandards/20190125_-_ITSA_-_Setting_Standards_for_Global-Token-Markets.pdf)

#### 4. Aplicaciones descentralizadas y organizaciones autónomas descentralizadas

Las aplicaciones descentralizadas (DApps) son “aplicaciones de *software* creadas a partir de contratos inteligentes, a menudo integradas con interfaces de usuario que utilizan tecnología web tradicional” (Wharton School, Digital Asset Project, World Economic Forum, 2020, p. 1). Desde una perspectiva tecnológica, se pueden definir como “una organización de contratos inteligentes orientados al consumidor, ejecutando una lógica de negocio predefinida dentro del entorno computacional transparente y determinista que ofrece una tecnología *Blockchain* pública” (Jensen et al., 2021, p. 46).

Al igual que las aplicaciones tradicionales, los servicios en DApp pueden emplear como canales la web o aplicaciones móviles. Sin embargo, se debe tener en cuenta que no todas las DApps ofrecen servicios financieros. Como se puede ver en la definición, pueden desarrollarse con finalidades no financieras (por ejemplo, juegos o apuestas).



Las principales diferencias entre las aplicaciones centralizadas y las descentralizadas radican en el uso de *Blockchain* y contratos inteligentes en sustitución de los sistemas de operaciones y contabilidad centralizados. Además, el almacenamiento de datos también es distribuido (*peer-to-peer network*) (Sunyaev et al., 2021, p. 13). Desde el punto de vista de infraestructura tecnológica existen distintos tipos de DApps en función de las capas de distancia a la propiedad de la cadena de bloques (Bit2me academy, 2022): (i) aquellas que cuentan con *Blockchain* propia y *tokens* propios, (ii) aquellas que operan sobre la *Blockchain* de un tercero y cuentan con *tokens* propios o del tercero, y (iii) aquellas que operan sobre DApps que operan sobre *Blockchain* de un tercero y cuentan con *tokens* de esa DApp o *tokens* propios.

Los requisitos para calificar como DApp pueden resumirse en (Johnston et al., 2020, pp. 2-12): (i) ser de fuente abierta y sin entidad específica que controle la mayoría de las fichas, (ii) operativa y contabilización en una *Blockchain* pública, (iii) sistema de acceso, contribución, pagos e incentivos basados soluciones criptográficas, y (iv) generación de fichas basadas en estándares criptográficos. Estas DApps son accesibles por cualquier persona que cuente con internet o un teléfono inteligente, siguiendo el principio de democratización de las finanzas independientemente del país en el que se encuentre la persona (Zetsche et al., 2020, p. 21), puesto que, para los protocolos DeFi, lo programado en el código es la ley, sin importar la jurisdicción desde la que se desarrolla o en la que se consume ese protocolo (Zetsche et al., 2020, p. 22).

Las DAO suponen la evolución de las DApp, dado que estas últimas todavía pueden acogerse a un modelo equiparable al de mutualidad, cooperativa, organización sin ánimo de lucro o incluso de fideicomiso anglosajón (*trust*). Según Buterin (2014), las DAO se definen como “una entidad que vive en Internet y existe de forma autónoma, pero también depende en gran medida de la contratación de personas para realizar ciertas tareas que la automatización por sí misma no puede realizar” (pp. 1-8).

El regulador europeo, en uno de los borradores de MiCA (versión de marzo 2022), definió estas organizaciones como “un sistema organizativo basado en reglas que no está controlada por ninguna autoridad central y cuyas reglas están enteramente encaminadas en su algoritmo” (borrador artículo 3.1 (1a) MiCA versión marzo 2022). Sin embargo, esta definición no fue incluida en la versión final del Reglamento.

En estas organizaciones, las reglas de gobernanza y decisión están marcadas por el protocolo que las creó y las personas lo acatan como elementos accesorios al protocolo,

que es el centro (*automation at the center, human at the edges*) (Buterin, 2014, pp. 1-8). Además, las DAO generan un valor intrínseco, que él denominó “capital interno”.

Las personas que trabajan en las DAO aportan de manera voluntaria, sin mediar contratos laborales, por lo que no se trata de una relación de exclusividad. Los beneficios que reciben los aportantes no son fijos, sino que se calculan en función del valor que le da la comunidad. Tampoco existen conceptos tales como propiedad industrial, propiedad intelectual o secreto empresarial en estos desarrollos, porque el trabajo es totalmente transparente y abierto. Desde el punto de vista de derecho laboral, este tipo de trabajos escapa del radar de los sistemas de cotización a la seguridad social, puesto que no existe una sociedad en sí. En todo caso, estos trabajadores podrían verse como autónomos y, por tanto, esos costos se trasladarían a la persona física.

Respecto a la forma societaria a la que se podrían asimilar las DAO, podría considerarse una variante de las tradicionales cooperativas<sup>84</sup>, dado que los dueños de los *token*, a su vez, son los que toman las decisiones de gobierno, mezclando, de este modo, propiedad con gobernanza de la organización. Sin embargo, debido a que sus miembros pueden encontrarse en geografías distintas, resultaría difícil identificar qué régimen legal les aplicaría (por ejemplo, si se tratara de una especie de *trust* anglosajón<sup>85</sup> o un *Verein* germano<sup>86</sup>).

En todo caso, la ausencia de forma legal definida por la organización podría generar el riesgo de que todos y cada uno de los dueños del *token* pudieran ser vistos como responsables legales en caso de incumplimientos regulatorios o contractuales. En caso de no establecer limitaciones a la responsabilidad, podría incurrirse, incluso, en responsabilidad a título personal. Por este motivo, fuera de la UE han comenzado a surgir iniciativas regulatorias en torno a qué clase de “envoltorio legal” debería de tener una DAO con el fin de limitar la responsabilidad de sus miembros (los denominados *legal wrapper*). Al tratarse de agrupaciones de individuos que, inicialmente, no tienen ánimo

---

<sup>84</sup> En el ordenamiento jurídico español, las cooperativas se definen como “una sociedad constituida por personas que se asocian, en régimen de libre adhesión y baja voluntaria, para la realización de actividades empresariales, encaminadas a satisfacer sus necesidades y aspiraciones económicas y sociales, con estructura y funcionamiento democrático, conforme a los principios formulados por la alianza cooperativa internacional, en los términos resultantes de la presente Ley” (artículo 1.1 de la Ley 27/1999, de 16 de julio, de Cooperativas).

<sup>85</sup> Los *trust* están contemplados en la regulación de Reino Unido mediante la *Recognition of Trusts Act* 1987 publicada el 9 de abril de 1987.

<sup>86</sup> En Alemania, el *Bürgerliches Gesetzbuch* (BGB) distingue entre dos tipos de *Verein*: (i) el *Nicht wirtschaftlicher Verein* o *Idealverein*, definido en el art. 21 como una asociación de fines no comerciales y (ii) el *wirtschaftlicher Verein* (art 22) con finalidad económica o comercial.

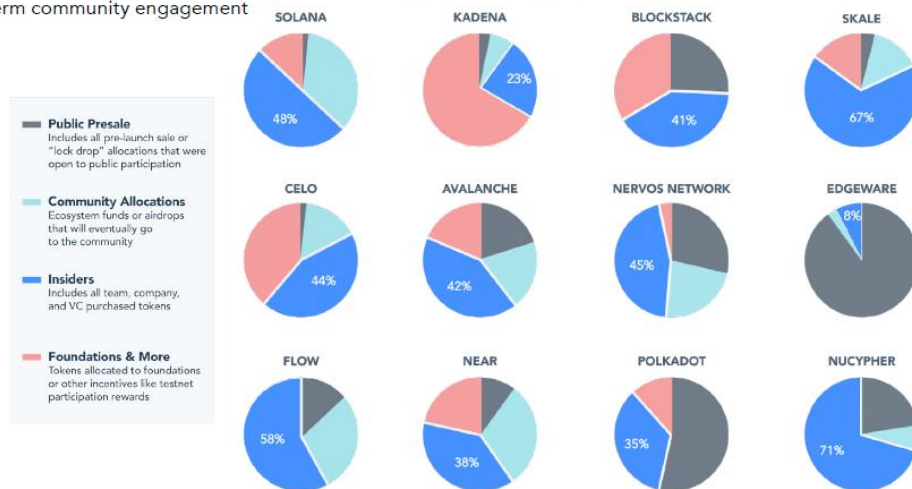
de lucro en la constitución de este tipo de organización, parece que la mayoría de los Estados que han regulado esta figura han optado por asimilarlas a la forma legal de las fundaciones. La alternativa a este tipo de encajes es el de la *Limited Liability Company* (LLC), que se identifica para las DAO constituidas en Wyoming, Marshall Islands (Legal Nodes, 2020) y Vermont (Guillaume y Riva, 2022, pp. 1-57).

Es discutible, incluso, la atribución de adjetivos tales como “descentralizado” o “autónomo” si en la práctica existen indicios de concentración o gobierno centralizado, tales como la concentración de fichas en una sola persona o entidad, la posibilidad de veto por parte de ciertos dueños del *token* o el hecho de que el voto de un número reducido de dueños sea equivalente de hecho a la decisión final o la imposibilidad de avance de la iniciativa. Esto podría definirse como indicios de centralización, similar a lo que sucede en el ámbito fiscal a la hora de identificar si una entidad tiene sustancia real en un país o no a efectos de tributación.

La concentración de votos o capacidades de veto puede reflejarse en los denominados *whitepaper* o libros blancos de los proyectos, que operan como documento base para explicar elementos como el negocio, los planes, la operativa, la gobernanza y los *tokenomics* (cómo funciona o genera beneficios financieros el proyecto). Un ejemplo de la concentración de gobernanza de los equipos fundadores y gestores (miembros del círculo cercano, incluyendo gestores, colaboradores y capital riesgo) frente al público en general puede evidenciarse en la figura 28, donde se observa que la acumulación de fichas por parte de miembros del equipo y fundadores suele ser muy superior al 50 % (casos de análisis de Solana, Kadena, Blockstak, Skale, Celo, Avalanche, Flow, Near y Nucypher).

## Pre-Launch Token Allocation Dedicated to Insiders vs. the Community

Distributing network capital and power more equitably at launch should enhance long-term community engagement



As of Oct 8, 2020 • Notes: Approx. amounts for some • Source: Messari, CoinList, Various blogs

Figura 28 Ejemplos de asignación de tokens y su distribución a octubre de 2020

Nota. Tomado de *Q-3 2020 Layer 1 review report*, W. Withian, 2020, Messari.

Otros ejemplos de posibles indicios de centralización podrían ser que el equipo que concentra votos se encuentre en una determinada jurisdicción. Bajo dicho panorama, podría plantearse la duda de si la responsabilidad recaería en los dueños de los *token* en general o en aquellos que hayan votado efectivamente respecto a una decisión que sea objeto de litigio. En caso de asimilarse a figuras normativas existentes, podría considerarse que se trataría de una situación similar a la de absentismo de accionistas y, por tanto, no eximiría de responsabilidad el no haber acudido a la votación de la decisión en concreto.

Una de las soluciones societarias que se han dado al problema ha sido el de reconocer a las propias DAO como una nueva fórmula de organización societaria. Estos casos, limitados a marzo de 2022, se concentran en Wyoming, Malta, Suiza, Estonia o Gibraltar (Ost, 2022, pp. 1-5). En lo que respecta a la caracterización de las DAO como organizaciones “autónomas”, el hecho de que la herramienta con la que los miembros de la organización votan es una solución fuera de la cadena de bloques, lo que requiere que una o varias personas ejecuten manualmente el resultado de la votación en la cadena, indicando una concentración de facultades o roles (Snapshot Labs, 2022, p. 1). Además, las gestiones de tesorería de las DAO también requieren de participación de roles equivalentes al de un director de tesorería o un director financiero.

Por último, hay que mencionar que este tipo de organizaciones también se enfrenta a retos en el diseño de la propia gobernanza. Esto se debe a que, en general, requiere del voto de sus miembros para la toma de decisiones, pero esta participación puede reducirse a lo largo del tiempo o en determinadas circunstancias, impactando en las cuotas de aprobación de las propuestas que se presenten; es decir, el número de miembros que votan no siempre es el mismo. Incluso, similar a lo que sucede en unas elecciones de partidos políticos, puede suceder que un porcentaje de los votantes no haya leído la propuesta o no la comprenda completamente. Por tanto, una de las mayores dificultades que se presenta en las gobernanzas de las DAO es cómo mantener o incentivar a sus miembros a lo largo del tiempo para que continúen votando.

No solo eso, sino que una inadecuada estrategia en el diseño de los *quorum* de decisión o en la asignación de *tokens* de gobernanza puede llevar a la instrumentalización de las propias DAO y sus protocolos por intereses propios, provocando alteraciones o manipulaciones de mercado. Este tipo de estrategias se denominan “ataques a través de una *dark* DAO”. Las DAO oscuras o *dark* DAO son agrupaciones (carteles) que adquieren *tokens* o compran votos de forma oculta con el fin de adquirir capacidad decisoria suficiente como para que la DAO atacada tome decisiones en favor de los intereses de la *dark* DAO debido a la pérdida control durante sus votaciones (Daian et al., 2018, pp. 1-13).

Como puede verse, las DAO plantean nuevas problemáticas de todo gusto y color, lo que hace surgir dos cuestiones de fondo: (i) si las DAO requieren de un régimen jurídico *ad hoc* que comprenda todas las cuestiones intrínsecas a la aparición de una nueva forma de agrupación basada en la tecnología, no vista hasta ahora; y (ii) reflexionar sobre el hecho de que las DAO son esquemas de gobernanza nativos del mundo descentralizado, no solo criptoactivos, sino también sobre los que descansan modelos de DeFi e incluso más allá de las finanzas como la Web 3.0 o el metaverso.

En este contexto, los criptoactivos y las DeFi descansarían sobre estructuras consideradas como esencialmente novedosas, por lo que las actividades por encima de ellas tendrían sus raíces en un instrumento normativo diferente y, por tanto, se estaría hablando de sustratos o esencias no del todo equivalentes. Este razonamiento llevaría a una potencial identificación de la necesidad de regular y supervisar todas estas actividades de forma distinta a lo visto hasta ahora. Respecto a si las DAO requieren de su propia ley marco y qué aspectos comprendería, ha de destacarse el trabajo de la Coalition of

Automated Legal Applications (COALA), cuyos miembros han desarrollado una comprensiva propuesta de ley modelo para las DAO (Coalition of automated legal applications, 2021, pp. 1-57).

Esta propuesta de ley modelo promueve la limitación de la responsabilidad de sus miembros bajo la condición de cumplimiento de determinados supuestos. Se diferencia de las propuestas actuales de envoltorio legal en el sentido de que no requiere asimilación a una forma societaria ya existente en los ordenamientos jurídicos (crea una agrupación no territorial que los Estados reconocerían con base en su adopción de la ley modelo o ley marco). Además, a diferencia de los casos actuales de las fundaciones sin ánimo de lucro, la propuesta diseñada identifica la capacidad de las DAO de tener fines lucrativos e incluso varios propósitos no comerciales en su artículo 1.

Otra importante diferencia es la ausencia del requisito de un capital mínimo (artículo 6) con base en la concepción de que una DAO es en todo momento transparente, por lo que sus acreedores podrán monitorizar en tiempo real su situación y salud económica. No solo eso, esta ambiciosa propuesta contempla, incluso, aspectos fiscales como el tratamiento de la DAO como un ente transparente en aquellos Estados que reconozcan la ley marco (artículo 20). De este modo, la tributación recaería directamente en sus miembros y se llevaría a cabo de acuerdo con la normativa del país en el que cada uno de ellos sea residente, salvando así la cuestión de la territorialidad.

La personalidad jurídica se reconocerá siempre y cuando cumpla con unas características técnicas descritas. De este modo, su cumplimiento implicará la responsabilidad limitada de sus miembros (artículo 5), salvo en casos de dolo o negligencia. Respecto a su gobernanza, el modelo propone distintos tipos de miembros con diversos derechos (presentar propuestas, votar, derechos económicos o combinaciones de los anteriores). Esta gobernanza debe reflejarse en los estatutos de libre acceso y legibles por cualquier individuo a través de interfaces gráficas de usuario (GUI, por sus siglas en inglés). En cuanto a la administración, cabe la posibilidad de designación de administradores o representantes legales para actividades no ejecutables de forma automática mediante *Blockchain* (artículo 14).

En general, estas propuestas se pueden dividir entre aquellos aspectos que se pueden asimilar a lo conocido y en los que se busca una cierta equivalencia (normativa y funcional), y aquellos aspectos identificados como esencialmente novedosos y que, por tanto, requieren de la determinación de nuevas soluciones.

Entre los ejemplos de paralelismos, se pueden encontrar equivalencias funcionales, como la emisión de acciones y la transmisión de acciones mediante tecnología (*Blockchain*), y similitudes legales, como la obligación de registro de la entidad con la finalidad de publicidad y efectos frente a terceras partes. Debido a que las DAO pueden desplegarse en una cadena de bloques, esta acción surtiría el mismo tipo de efecto y, por consiguiente, no necesitaría de la obligación de registro.

En relación con los aspectos diametralmente novedosos, el Capítulo V (artículos 16-18) de la ley modelo plantea posibles soluciones a escenarios no conocidos hasta ahora en el plano societario, como los casos de bifurcaciones duras o contenciosas de cadenas de bloques (*hard forks o contentious fork*)<sup>87</sup>, modificaciones, actualizaciones de protocolos, migraciones y sus implicaciones para el negocio y los miembros de la DAO, así como para los usuarios. También aborda los casos de eventos de fallo y el tipo de responsabilidades contempladas. De esta forma, tratan de acometer dudas actualmente abiertas, como qué sucede con la DAO “entidad jurídica” si la *Blockchain* sobre la que descansa y opera sufre un bifurcación dura, existiendo acuerdo o desacuerdo de la comunidad si migrar o no a la nueva versión.

Como se puede observar, las DAO plantean elementos no antes vistos ni abordados en los ordenamientos jurídicos, por lo que cabe concluir que una simple extensión o intento de adaptación en los modelos existentes no será suficiente, dado que una ley marco o una solución similar sería el camino más adecuado. Por ello, en este caso se identifica un claro ejemplo de laguna normativa sobrevenida que no puede cubrirse mediante la analogía y que, bajo esta perspectiva, es probable que desemboque en una regulación marco o una modificación de las normativas regulatorias de la UE para brindar seguridad jurídica a estos nuevos tipos de agrupaciones.

Derivado de ello, la segunda reflexión parece indicar que el tratamiento de actividades y servicios que descansan con base en estos modelos, especialmente aquellos referidos a las finanzas como los criptoactivos y las DeFi, requerirán de sus propios entornos normativos y de supervisión como soluciones distintas a los esquemas que se venían aplicando hasta ahora. Esta argumentación se desarrolla en profundidad en la segunda parte de esta tesis.

---

<sup>87</sup> La ley marco define los *hard fork* como una bifurcación dura que resulta en dos cadenas de bloques divergentes y potencialmente competidoras (art. 3 (6)).

### III. FINANZAS DESCENTRALIZADAS (DEFI)

#### 1. Finanzas descentralizadas (DeFi) y su propósito

Las DeFi son la siguiente variación del mundo *FinTech* que actualmente se encuentra en expansión. En ese sentido, las *FinTech* son un puente entre las finanzas tradicionales y el futuro descentralizado. Esto se debe a que la mayoría de las *FinTech* todavía operan bajo modelos basados en el tercero de confianza o en colaboración con instituciones financieras tradicionales mediante modelos de banca abierta, en la que los usuarios autorizan compartir datos financieros con entidades terceras (generalmente *FinTech*) (Pérez, 2019, p. 143).

En general, aún emplean monedas de curso legal o son plataformas de intercambio entre dichas divisas y los criptoactivos. Por otra parte, dependiendo de su actividad, pueden operar en actividades que requieran licencia o registro ante las autoridades de las jurisdicciones en las que operen. Por último, se trata de entidades con personalidad jurídica propia, por lo que se sujetan a las regulaciones propias y a regímenes de responsabilidades en casos de incumplimientos regulatorios.

En contraste, las DeFi buscan operar basadas en la confianza en las reglas de la tecnología *Blockchain*, prescindiendo de los costes que suponen los intermediarios financieros. Además, bajo estos protocolos, las personas vuelven a recuperar el control de sus activos y de sus finanzas, no requiriendo de instituciones financieras, bancos centrales o monedas oficiales cuyo valor fluctúa en función de las políticas monetarias centrales (Caballero et al., 2020, p. 66-70).

Las DeFi se pueden definir como “la prestación descentralizada de servicios financieros a través de cualquier combinación de infraestructura, mercados, tecnología, métodos y aplicaciones” (Zetsche et al., 2020, pp. 173-174). Desde una perspectiva tecnológica, las DeFi son un “nuevo tipo de aplicaciones financieras abiertas implementadas en cadenas de bloques sin permisos y de acceso público” (Jensen et al., 2021, p. 1).

Dependiendo de la actividad, criptoactivo empleado y del nivel de descentralización detrás de las organizaciones que ofrecen el servicio, puede llegarse al caso de que no exista una entidad o persona responsable o identificable, solo un *smart contract*. Esto genera que no esté claro el organismo supervisor, si la actividad está regulada o quién



será la persona o entidad responsable en casos de incumplimiento. Las DAO, estudiadas anteriormente, pertenecen a tipo de estructuras plenamente desconcentradas.

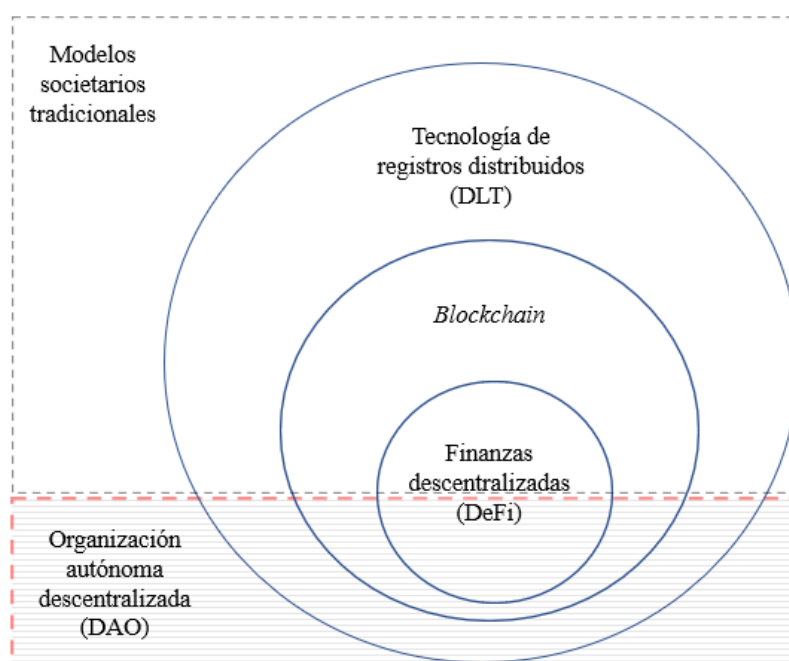


Figura 29. Gráfico de relación de modelos societarios y nuevas tecnologías

Nota. Elaboración propia.

Como se observa en la Figura 29, las DeFi son una subcategoría dentro de *Blockchain* y, a su vez, son una subcategoría dentro de la DLT. Asimismo, no todos los modelos operativos de DeFi operan bajo estructuras de DAO, sino que también pueden darse modelos societarios tradicionales. En ese orden de ideas, cabe deducir que las DeFi abarcan todo un ecosistema heterogéneo de actividades que incluyen no solo versiones evolucionadas del mundo ya conocido, y nuevos modelos financieros propios del mundo DeFi, sino también una infraestructura operacional y tecnológica completamente paralela a la existente en la actualidad. Las DeFi se caracterizan por los siguientes elementos:

Primero, el uso de protocolos automatizados de compensación y liquidación (World Economic Forum [WEF], 2021, pp. 5-38) que potencia el prescindir de figuras tradicionales del mundo financiero, como pueden ser las entidades depositarias (CSD) para el caso de instrumentos financieros.

Segundo, en relación con el apunte previo, este tipo de finanzas pueden diseñarse prescindiendo de la figura de custodio o tercero de confianza (World Economic Forum [WEF], 2021, pp. 5-38).

Tercero, DeFi aporta la característica nativa de universalidad o disponibilidad global constante, sujeto a la provisión de acceso a internet (PricewaterhouseCoopers International Limited, 2021, p. 7). Esto no deja de suponer un absoluto reto regulatorio y supervisor, dado que los perímetros regulatorios son limitados y estos modelos los desbordan. No solo eso, sino que la operativa es incensurable, dado que, una vez puesta en producción, no puede alterarse ni cerrarse por los gobiernos. En consecuencia, se habla de irreversibilidad de las operaciones. Por otro lado, también supone un reto operativo, puesto que los mercados que hasta ahora operaban con rangos horarios (horas de corte de operativa) ahora compiten con un modelo de mercado digital descentralizado operativo 24 horas al día, siete días a la semana, durante todo el año.

Cuarto, DeFi ofrece la posibilidad de una arquitectura tecnológica programable, abierta y apilable o de “lego” (World Economic Forum [WEF], 2021, pp. 5-38), por lo que resulta más fácil construir y desarrollar ideas de negocio financiero. Además, esta arquitectura es transparente en el caso de las cadenas de bloques públicas, permitiendo que cualquiera pueda auditar su código y operativa (PricewaterhouseCoopers International Limited, 2021, pp. 5-25). La cuestión, sin embargo, es quién cuenta con el conocimiento suficiente para llevar a cabo análisis forenses de la robustez del código.

Quinto, ligado al punto anterior, ha de apuntarse que esta innovación está basada en la apertura e intercambio de información (Meegan y Koens, 2021, p. 5), esto es, modelos colaborativos que se muestran en el aumento de soluciones de interoperabilidad entre cadenas (por ejemplo, los denominados “puentes”) y aplicaciones (PricewaterhouseCoopers International Limited, 2021, pp. 5-25).

Sexto y último, “el código es la ley”. Es decir, prescinde de las tradicionales estructuras normativas, jurídicas y de supervisión dentro de las que venían operando hasta ahora las entidades que ofrecían servicios financieros.

Es precisamente esta combinación de factores la que hace plantear la necesidad de desarrollo de un nuevo paradigma en la legislación (cripto-legislación) y, por tanto, derecho. Esto da cabida al denominado cripto-derecho, que englobaría la necesidad del desarrollo de soluciones regulatorias no solo de criptoactivos y DeFi, sino también de la tecnología y programas subyacentes a estos, esto es, *Blockchain* y contratos inteligentes (García, 2018, pp. 94-102).

## **2. Evolución de CeFi a DeFi y el cambio en la figura del tercero de confianza**

Los modelos financieros tradicionales se basan en el uso de terceros de confianza para la perfección de las operaciones (Zetsche et al., 2020, p. 7-10). De esa manera, se habla de puntos de concentración o modelos centralizados que aglutinan las operaciones o las tomas de decisiones. A su vez, estos puntos de concentración suponen focos de riesgo, por lo que la fuerza normativa y supervisora se centra en ellos con mayor o menor exigencia en función de su nivel de materialidad, siguiendo un enfoque de proporcionalidad. Sin embargo, las crisis del sector económico han ido derivando en mayores requerimientos regulatorios que a menudo se han ido desarrollando a nivel local y, por consiguiente, han provocado una fragmentación de criterios normativos.

Es precisamente debido a esta situación que surge la filosofía de las finanzas lideradas por la tecnología (Zetsche et al., 2020, pp- 7-10), para reducir los errores o las malas prácticas provocados por los humanos (no solo instituciones financieras, sino también gobiernos y reguladores).

Como se indicó en las características, los modelos DeFi dicen ser patrones en los que se prescinde del elemento de un tercero en el que las partes confían. Sin embargo, esto no es del todo cierto, puesto que la decisión de empleo de un protocolo u otro implica la confianza en este y en el desarrollador o desarrolladores que lo hayan creado. Es decir, se produce un desplazamiento de la certeza hacia perfiles de corte tecnológico o con cierto nivel de conocimientos como para poder desarrollar los protocolos en *Blockchain*. El público, el usuario, confía en el código (que este no sea *hackeado* y que no tenga errores de programación), pero desconoce el nivel de conocimientos y experiencia del desarrollador de este, no solo desde el punto de vista tecnológico, sino también financiero.

## **3. Niveles de descentralización**

Puede pensarse que las CeFi y las DeFi son solo dos opciones, pero similar al caso del blanco y el negro, existen escalas de grises entre un extremo y el otro, que se pueden catalogar en función del nivel de independencia que tiene el usuario sobre sus activos y operaciones (Qin et al., 2021, p. 2).

El extremo centralizado se caracteriza por los activos que se encuentran custodiados por un tercero (generalmente supervisado por una autoridad central del país o región). Este tercero requiere una serie de documentos e información para considerar si acepta

realizar negocios con el usuario o no. Además, tiene la capacidad de rechazar o bloquear las operaciones solicitadas por el usuario, basándose en su apetito de riesgos de impago, fraude, blanqueo de capitales o sanciones financieras internacionales. Por tanto, el usuario tiene un alto nivel de dependencia de terceros que fijan las reglas del juego.

Los niveles de dependencia intermedios serían escenarios en los que el usuario puede custodiar por sí mismo el activo, pero que, a la hora de operar, sigue dependiendo de los criterios de la institución, quien puede rechazar o bloquear la operación (por ejemplo, basándose en su apetito a riesgos de crimen financiero). La independencia y, por tanto, la entrada en el mundo de las DeFi se da cuando los usuarios tienen capacidad de acceder al servicio por sí mismos (sin ningún tipo de filtro), custodiar por sí mismos los activos y operar sin la intervención de criterios humanos, teniendo en cuenta que las reglas establecidas en los protocolos en los que opera no puedan ser alteradas por grupos de interés o control; es decir, que incluso la estructura de gobernanza y toma de decisiones de cambios tecnológicos no esté concentrada.

Los servicios DeFi pueden lanzarse o modificarse de diversas formas en función de los esquemas de gobernanza (World Economic Forum [WEF], 2021, p. 9): desde sistemas de gobierno centralizados, en los que una entidad o desarrollador tiene la capacidad de tomar decisiones y cambiar el servicio, hasta sistemas de voto por parte de los dueños de *tokens* de gobernanza<sup>88</sup>, pasando por sistemas híbridos en los que los desarrolladores de la DApp mantienen ciertos privilegios y los dueños de los *tokens* de gobernanza tienen capacidades limitadas.

Finalmente, los niveles de centralización o descentralización pueden ser distintos entre categorías que conforman el protocolo, es decir, gobernanza, capacidad de modificación del protocolo, custodia de activos y ciberseguridad (World Economic Forum [WEF], 2021, pp. 5-38). Igualmente, caben distintos diseños entre protocolos que se dediquen al mismo vertical. Debido a este complejo esquema modular, es difícil establecer estándares y, por tanto, a coyunturas de control o supervisión eficientes.

---

<sup>88</sup> Los *tokens* de gobierno o fichas de gobernanza son criptoactivos fungibles (intercambiables) que implementan una lógica de votación entre una serie de partes interesadas. Por medio de este tipo de *tokens*, sus propietarios pueden participar en la toma de decisiones que impactan en el desarrollo del protocolo al que los *tokens* pertenezcan (Jensen et al., 2021, p. 2.). Los esquemas y requisitos de mayorías dependerán de las reglas del protocolo.

#### 4. Las nuevas contrapartes

En línea con lo anterior, el mundo de las DeFi prescinde de figuras conocidas, como los bancos centrales y la banca comercial. Además, las organizaciones autónomas descentralizadas obvian los conceptos societarios convencionales de accionistas o consejo de administración. Esta tesis postula que esto no significa que estos roles no existan, sino que evolucionan hacia nuevos perfiles; es decir, estas actividades no se destruyen, sino que se diluyen o se transforman. En la Tabla 10 se exponen ejemplos del traspaso del rol tradicional en las DeFi.

Tipo	Actividad	Rol tradicional	Posibilidades en finanzas descentralizadas
Macroeconómico	Emisión de dinero	Bancos centrales, bancos comerciales, emisores de dinero electrónico	Desarrollador de protocolos (piezas clave), equipo gestor emisor de criptoactivo
Macroeconómico	Política monetaria	Bancos centrales	Lógica del contrato inteligente
Macroeconómico	Control de liquidez en el mercado	Bancos centrales, inversores.	Proveedores de liquidez y liquidadores
Societario	Propiedad	Accionistas	Nodos mineros, equipo desarrollador, dueños de <i>tokens</i> , fundadores
Societario	Gobernanza	Consejo de administración u equivalente	Nodos mineros, equipo desarrollador, dueños de <i>tokens</i> , fundadores
Financiero	Provisión de servicios financieros	Entidades financieras y <i>FinTech</i>	Proveedores de interfaz, protocolos DeFi
Financiero	Confianza o validación de operación	Personal de entidades financieras (operador)	Nodos validadores
Financiero	Servicios auxiliares o conexos	Entidades financieras y <i>FinTech</i>	Oráculos, protocolos auxiliares

Tabla 10. Ejemplos de actividades en roles tradicionales y su equivalente en las finanzas descentralizadas

Nota. Elaboración propia.

A continuación, se resumen brevemente las principales contrapartes DeFi que han suplido figuras tradicionales.

El primer rol identificado es el de el desarrollador, equipo gestor y emisores: los desarrolladores, entendidos como generadores de piezas clave del protocolo, pasan a ser los diseñadores e implantadores del equivalente a las infraestructuras de pago en el mundo centralizado. Asimismo, acumulan nuevos cometidos, como el diseño de nuevos productos y servicios o la emisión de nuevos criptoactivos. Incluso, dependiendo del

diseño de los protocolos, se confieren capacidades de acumulación de *tokens* de gobernanza, por lo que en ciertas ocasiones pueden tener capacidad de veto.

En determinados casos, como puedan ser los de los involucrados en la ideación y puesta en práctica de criptomonedas estables algorítmicas, están encargados del diseño de la lógica que regirá la provisión de criptoactivos de un determinado tipo en el mercado (creando o destruyendo en función de la demanda) y, por tanto, llegan a tener una función similar al de los bancos centrales respecto a las decisiones de políticas monetarias.

Por lo anterior, el papel de estos agentes en la actualidad ha llegado a ser más relevante de lo que era en el pasado. En este sentido, comienzan a verse casos de responsabilidad penal de desarrolladores, como el de Alexey Pertsev, desarrollador de la aplicación denominada Tornado Cash, que se catalogó como de riesgo de crimen financiero y se incluyó en la lista de contrapartes sancionadas por la Oficina de Control de Activos Extranjeros americana (OFAC). Pertsev, a su vez, fue acusado de facilitar el blanqueo de capitales por su trabajo en esta aplicación (Schickler, 2022, pp. 1-3).

Dentro de este concepto de desarrollador pueden incluirse diversos perfiles con diferentes responsabilidades y con esquemas de relación contractual poco claros (Commission de Surveillance du Secteur Financier [CSSF], 2022, pp. 16-18), los cuales se indican a continuación:

Desarrollador de la cadena de bloques: se encarga principalmente de crear el código, las nuevas funcionalidades, las mejoras o las remediación de deficiencias detectadas sobre la cadena de bloques. En general, trabajan sobre fuentes abiertas (*open source*), por lo que no cobran por su esfuerzo y, por tanto, no existe una relación contractual, dado que es un trabajo voluntario que se comparte por la comunidad y puede ser aprovechado o modificado por otras contrapartes.

Proveedor de servicios de infraestructura: se trata de las contrapartes que proveen de la infraestructura necesaria para que la cadena pueda operar. Por lo general, se consideran bajo este esquema los denominados nodos, los cuales se describen con mayor profundidad a continuación. En cuanto a DLT abiertas, estos agentes no cuentan con una relación contractual, por lo que participan voluntariamente a cambio de esquemas de incentivos.

Proveedor de soluciones: los proveedores de soluciones diseñan el *software* o la aplicación para los usuarios intermedios y finales. Para ello, se basan en la tecnología *Blockchain*, pero incluyen en su solución pantallas que pueden ser entendidas y

explotadas por los usuarios. En este caso, se trata de un proveedor de servicios, pero por lo general no se identifican acuerdos contractuales más allá de la aceptación de términos y condiciones de uso de su plataforma.

El segundo gran concepto es el de nodo. Los nodos son los equipos que se ponen al servicio de la *Blockchain*, actualizando y manteniendo las acciones (Guaita et al., 2019, pp. 5-160) que se autorizan de forma segura y descentralizada, sincronizándose entre ellos. Existen distintos tipos de nodos:

- a) Nodos parciales o ligeros: son aquellos que usan los criptoactivos, pero no los minan, verifican o mantienen copia completa de la *Blockchain*, puesto que no se ha descargado el *software* necesario para ello (por ejemplo, casos de simples billeteras cripto). Dependen de un tercero (los supernodos) para operar y recibir la información.
- b) Nodos completos: son los que encajan con la definición propiamente dicha, dado que obtiene una copia de la *Blockchain* en sus equipos al haber descargado el *software* (Caballero et al., 2020, p. 81). Dentro de esta categoría se encuentran, en función de los mecanismos de consenso que se aplique, los nodos mineros (equipos que mantienen una copia completa y ejecutan *software* de minería que permite anotar transacciones en el bloque y verificarlos), los nodos validadores (aquellos que tienen en cuenta el número de *tokens* que posee el nodo y tiempos de conexión, entre otros) y los nodos de autoridad (los bloques son verificados por nodos que han sido previamente evaluados y aprobados).
- c) Supernodos: son nodos completos que operan como elemento de conexión continua, abierta y pública entre nodos, incluyendo los parciales.

El tercer gran concepto son los proveedores de liquidez. Al igual que en las CeFi, en el contexto de las DeFi es necesario recurrir a fuentes de liquidez. Sin embargo, si bien en los modelos tradicionales la liquidez proviene de los propios bancos centrales o de los depósitos del público en las instituciones financieras, en el escenario de las DeFi surge la figura de los proveedores de liquidez, que aportan sus criptoactivos en forma de depósito a las piscinas de liquidez o reservas de liquidez. Estos depósitos, bloqueados en contratos inteligentes, tienen incentivos para estos proveedores de liquidez mediante comisiones, intereses o fichas. No hay requerimientos o barreras en la actualidad para ser un proveedor de liquidez, por lo que cualquier persona que cuente con los fondos podrá llevar a cabo esta actividad.

El cuarto concepto se relaciona con los dueños de fichas que pasan a ser los responsables de la gobernanza del producto o servicio DeFi. Cuentan con la capacidad de cambiar las reglas de incentivos o criterios propios del protocolo. A modo de ejemplo, en el caso de las casas de cambio descentralizadas (también llamadas DEX), los dueños de los *tokens* pueden proponer y votar el incluir nuevas criptomonedas dentro de su oferta de criptoactivos. En general, los dueños de las fichas pueden ser miembros del equipo fundador, mineros o personas que han adquirido *tokens* por aportar liquidez o simplemente los han comprado.

Finalmente, están los usuarios (Commission de Surveillance du Secteur Financier [CSSF], 2022, pp. 16-18) que, a su vez, podrían dividirse entre usuarios intermedios o corporativos y usuarios finales. Esto se debe a que los servicios de proveedores de soluciones pueden enfocarse en las instituciones del mundo centralizado (por ejemplo, instituciones financieras o *FinTech*) que ofrecen servicios al público en general. En estos casos, suele existir una relación contractual entre las partes, siendo el modelo más común el de proveedor de servicios de *software*.

Los usuarios finales pueden consumir servicios a través de los usuarios intermedios o corporativos anteriormente indicados, o directamente de los proveedores de soluciones. Para los primeros suele existir una relación contractual de provisión de servicios. En el supuesto de los segundos, la relación contractual no está clara, pudiendo existir o no, y, por lo general, limitándose a la aceptación de términos y condiciones de uso de la plataforma.

Cabe aclarar que estos roles no son excluyentes entre sí (Commission de Surveillance du Secteur Financier [CSSF], 2022, p. 19), sino que, la misma contraparte juega varios papeles en el mundo descentralizado, lo que, en ocasiones, puede derivar en conflictos de interés en los negocios que en la actualidad no cuentan con medidas de control o algún tipo de limitación. Debido a esta dilución o transformación de roles, las autoridades se enfrentan a la necesidad de un cambio en su forma de percibir la producción de marcos normativos y estrategias de supervisión, como se analiza más adelante.

## **5. Infraestructura**

La infraestructura del ecosistema de DeFi cuenta con varias capas con diferentes finalidades (Schär, 2021, pp. 1-22) y enfocados en distintas contrapartes. Estas piezas



pueden catalogarse en cuatro grandes grupos de mayor a menor cercanía desde el punto de vista de los usuarios y consumidores de los servicios DeFi:

La primera categoría de cercanía al público general se encuentran las aplicaciones (tanto centralizadas –App– como descentralizadas –DApp–) e interfaces de usuario. Dentro de este primer nivel, se localizan las aplicaciones a las que tiene acceso el público común. Incluye, principalmente, servicios puente entre el mundo financiero tradicional y los ecosistemas DeFi (billeteras digitales y casa de cambio de divisas de curso legal por cripto y viceversa, que sirven como punto de entrada y salida).

Además, en este nivel se hallan las aplicaciones e interfaces desarrollados para un servicio granular en concreto de nicho, cuya característica es la especialización mono-producto. En contraste con estas, también se identifican aplicaciones con una finalidad de agrupamiento de las anteriores, para poder comparar, agregar servicios o permitir una mejor gestión de las inversiones y patrimonio. Estas aplicaciones e interfaces están unidos o agregados a protocolos del segundo nivel. Actualmente, ciertas Apps y DApps de usuarios tienen la capacidad de agrupar distintas *Blockchain* para mayor comodidad de los usuarios.

En el segundo estadio se encuentran los protocolos y servicios para desarrolladores. Los protocolos permiten la creación de estándares para los servicios, los cuales se implementan a través de contratos inteligentes (Schär, 2021, pp. 1-22). También se incluyen servicios o piezas auxiliares para los desarrolladores, como componentes de identidad, control de crimen financiero, los oráculos para la comprobación de condiciones y precios, entre otros. Los oráculos son uno de los elementos de análisis posterior debido a la novedad de esta figura respecto a las finanzas tradicionales.

En un tercer bloque se identifican a los criptoactivos, ya sean los propios de la *Blockchain* de la que se esté tratando (nativos), *tokens* o fichas emitidos bajo los estándares de la DLT (en Ethereum son los ERC-20 y ERC-721, principalmente), distinguiendo entre fungibles como las criptomonedas, y los no fungibles como los relacionados con el arte (NFT) (Schär, 2021, pp. 1-22). En esta capa también se incluyen las soluciones de *tokens* que representan a criptoactivos que provienen de otra *Blockchain* (denominados servicios de envoltorio o *wrapper services*). Por ejemplo, *bitcoin* tiene su propia *Blockchain*, y para operar en el ecosistema de Ethereum, que es una DLT distinta, se debe hacer mediante este tipo de protocolos. En el protocolo BitGo, se bloquean

*Bitcoins* como depósito para que se emitan los denominados *wrapped bitcoin* o *wBTC*, que son *tokens* en formato ERC-20.

Recientemente, surgió un nuevo tipo de fichas, los ERC-1155, los cuales cuentan con el potencial de añadir aún más retos jurídicos y de control a los propios de las DeFi, dado que los *tokens* diseñados bajo este formato tienen la capacidad de generar *tokens* con las características de criptomonedas, NFT o ambos (Bit2me Academy, 2023, pp. 1-7).

Finalmente, se encuentra el nivel de liquidación, representado por la propia ficha nativa y la *Blockchain*, funcionando como sistema operativo y contable. Funciona como cimiento del total de la infraestructura DeFi, incluyendo la base de las reglas de la operativa dentro de esta y operando como mecanismo de partida respecto a la seguridad, propiedad o disputas (Schär, 2021 , pp. 1-22).

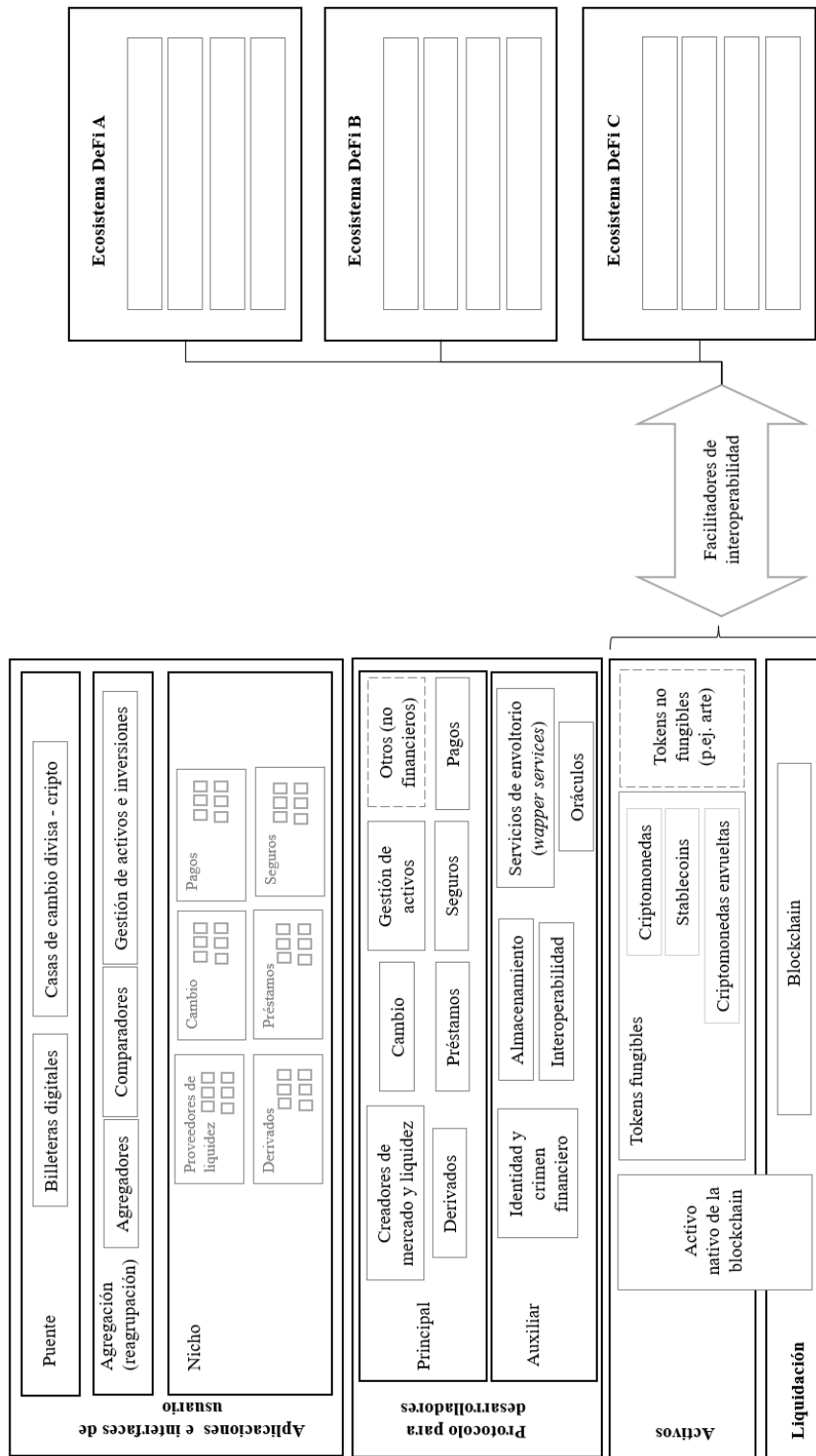


Figura 30. Infraestructura modelo del ecosistema de finanzas descentralizadas (DeFi) y su interoperabilidad con otros ecosistemas

Nota. Tomado de *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, por F. Schär, 2021, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3571335](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335)

## IV. CRIPTOMONEDAS O CRIPTODIVISAS

### 1. Activos digitales: criptoactivos y criptomonedas

A menudo se habla indistintamente de activos digitales, criptoactivos y criptomonedas; sin embargo, se trata de conceptos diferentes. Los activos digitales son un tipo de activos que engloban a los criptoactivos, criptomonedas y *tokens*, entre otros. Pueden definirse como “representaciones digitales de valor habilitados por la criptografía y la tecnología de registros distribuidos” (Su, 2020, pp. 2-24). Los activos digitales abarcan representaciones en *Blockchain* de todo tipo de activos y derechos, incluyendo, a modo de ejemplo, instrumentos financieros tradicionales, inmuebles, obras de arte o música.

Por otro lado, en el contexto de la UE, MiCA en su artículo 31, 5), define a los criptoactivos como “una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar”. Sus principales características han sido descritas por la EBA (European Banking Authority [EBA], 2019c, pp- 10-11). Primero, dependencia de criptografía, tecnología de registros distribuidos o análoga como parte de su valor añadido; segundo, no ha sido emitido o garantizado por un banco central o autoridad; y, tercero, puede emplearse como una forma de intercambio de valor, inversión o acceso a bienes y servicios.

Estos elementos característicos, si bien podían ser válidos en 2019, en la actualidad requieren de ciertas precisiones. La primera de ellas es que, hoy en día, se están desarrollando numerosos proyectos de emisión de monedas de bancos centrales basadas en la criptografía y que podrán emplearse como un forma de intercambio de valor e inversión. Por tal motivo, la característica de no haber sido emitido o garantizado por un banco central o autoridad debería reemplazarse por una división de criptomonedas de emisión privada versus criptomonedas de emisión pública, siguiendo la clasificación general propuesta por Barrio et al. (2021) (Barrio et al., 2021, pp. 53).

La segunda precisión que se debe realizar es que, en 2021, los criptoactivos también englobaban la capacidad de decisión dentro de las DAO, por lo que la tercera característica ha de incluir que los *tokens* pueden ser una forma de acceso a la gobernanza de las DAO. Asimismo, los *tokens* pueden llegar a representar propiedad sobre activos físicos e incluso la identidad digital de las personas en el mundo descentralizado.

Los criptoactivos pueden ser fungibles (criptomonedas o criptodivisas) o no fungibles (como es el supuesto de uso de *Blockchain* con fines artísticos). En ese sentido, las criptomonedas son un subconjunto de criptoactivos divisibles, intercambiables, portátiles y consumibles. En lo concerniente a las criptomonedas o criptodivisas, las más conocidas en la actualidad son *bitcoin*, por suponer el nacimiento de las criptomonedas, y *ether*, por ser el *token* de la *Blockchain* Ethereum, que aporta mayor valor al permitir ofrecer servicios descentralizados.

## **2. Criptomonedas de emisión privada**

Las criptomonedas de emisión privada (el término más preciso sería criptoactivos fungibles con finalidad financiera) han experimentado un incremento brusco a lo largo de los últimos años debido a que, en DeFi, cualquier persona en el mundo tendría la capacidad potencial de desarrollar su propia criptomoneda. Debido a ello, y con el fin de priorizar casos de materialidad, esta sección se centra en las dos principales criptomonedas generadas por las dos *Blockchain* más conocidas y usadas, esto es, *bitcoin* y *ether*. También se aborda un tipo de criptoactivos de emisión privada y mayor estabilidad, el cual ofrece mayor potencial como medio de pago: las denominadas *stablecoins* o monedas estables.

### **2.1 Bitcoin**

*Bitcoin* se define de la siguiente manera:

*Moneda digital, criptográfica y descentralizada que nace con el propósito de ofrecer un sistema alternativo que no requiere que confiemos a nadie los derechos de manipular las propiedades del activo que utilizamos como dinero ni la capacidad que tenemos para guardarlo y transferirlo, ya que nadie tiene el poder de alterar las normas inicialmente establecidas.* (Caballero et al., 2020, p. 77)

La idea de *bitcoin* como moneda y medio de pago alternativo al sistema financiero tradicional vio la luz en 2008 a través de un artículo denominado *Bitcoin: a peer-to-peer electronic cash system* (Nakamoto, 2008, pp. 1-9). De este modo, Nakamoto (pseudónimo empleado por el autor o autores) esbozó un sistema que prescinde del tercero de confianza, con operativa prácticamente inmediata independientemente del país en el que se encuentren las partes, y que cuenta con una robusta seguridad frente a ataques o intentos de control de los países (Caballero, 2019, pp. 81-91).

*Bitcoin* se diseñó a partir de un modelo de PoW y con un límite de cantidad de emisión fijada en 21 000 000 *bitcoins* (Caballero et al., 2020, pp. 86), por lo que se basa en un modelo financiero deflacionario. Este mecanismo de consenso consume altas cantidades de energía desde el punto de vista de trabajo computacional, lo que provoca que la validación de los bloques lleve tiempo y que haya recibido críticas desde el punto de vista de la capacidad operacional. Sin embargo, estos inconvenientes son compensados por unas características inherentes a la *Blockchain* sobre la que corre la criptomoneda, esto es, la resistencia a ataques, tal y como apuntó Morales (Morales, 2018, pp. 55). Sin embargo, no todo son ventajas en esta criptomoneda, dado que, debido a su naturaleza, cuenta con limitaciones que se encuentran bajo discusión, como la capacidad de la infraestructura (potenciales cuellos de botella en casos de uso masivo de bitcoin) o su alta volatilidad.

Por otro lado, existen características de la moneda que tienen un doble filo como su anonimato, que puede verse como una forma de protección de los datos personales en casos de transacciones financieras internacionales, pero que, a su vez, son un riesgo a la hora de controlar y prevenir el blanqueo de capitales y financiación del terrorismo.

En cuanto a la definición de la naturaleza jurídica de las *bitcoin* y, por ende, los criptoactivos, esta se describe en la sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª) número 326/2019, de 20 de junio, en la que se indica claramente que estas no tienen consideraciones de dinero de curso legal, ni tampoco son un activo material. En concreto, indica lo siguiente:

*[...]no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin.*

*Aun cuando el precio de cada bitcoin se fija al costo del intercambio realizado, y no existe por tanto un precio mundial o único del bitcoin, el importe de cada unidad en las diferentes operaciones de compra (por las mismas reglas de la oferta y de la demanda), tiende a equipararse en cada momento.*

La controversia sobre si el *bitcoin* se considera un instrumento de inversión o un medio de pago se analiza desde el punto de vista de sus implicaciones fiscales en el caso

Skatteverket vs. Hedqvist<sup>89</sup> en dicha sentencia, donde el Tribunal de Justicia de la UE dejó claro que el *bitcoin* es un medio de pago empleado de forma similar a cualquier medio de pago legal, pero que solo tiene validez con previo acuerdo de las partes. Por tanto, no puede interpretarse como una propiedad tangible del artículo 14 de la Directiva IVA<sup>90</sup> y no es un valor que confiere un derecho de propiedad, un instrumento financiero, ni una garantía de naturaleza comparable. El fallo concluye que los servicios de intercambio de *bitcoin* por dinero de curso legal se interpretan como exentos del impuesto de valor añadido.

Sin embargo, cabe argumentar que el uso tanto de *bitcoin* como *ether* (criptomoneda que se aborda a continuación) es mayormente especulativo. Precisamente, la volatilidad de su valor hace que, en la práctica, considerar *bitcoin* o *ether* como instrumento de pago estable (equivalente al dinero de curso legal) sea poco viable.

## 2.2 *Ether*

*Ether* es la criptomoneda propia de la red Ethereum. Ethereum surgió como una progresión de *Bitcoin* en 2013 de la mano de Vitalik Buterin (Ethereum, 2021a, pp. 1-36). Se trata de una variación, puesto que Ethereum no solo es un corredor de pago con criptomoneda propia de la cadena de bloques, sino que incorpora el concepto de contratos inteligentes y, con él, abre la puerta a la creación de DApps y DAO. A su vez, Ethereum permite no solo transaccionar con *ether*, sino también crear otro tipo de criptoactivos, ya sean monedas o *tokens* no fungibles (NFT)<sup>91</sup>. Incluso, crea formas de uso de monedas de otras *Blockchain* en Ethereum. Un ejemplo de ello son los wBTC, ya mencionados, o la representación de instrumentos financieros en la *Blockchain* (instrumentos financieros *tokenizados*).

En contraste con *bitcoin*, *ether* no cuenta con un número limitado de unidades (es un modelo inflacionario) y sus validadores (rol similar al de los mineros en *bitcoin*) pueden cobrar tarifas por confirmar las transacciones; es decir, las transacciones tienen un costo, denominado *gas*, en función de la complejidad del contrato inteligente sujeto a validación.

---

<sup>89</sup> Sentencia del Tribunal de Justicia de la Unión Europea del 22 de octubre de 2015, respecto al tratamiento fiscal de los servicios de *exchange cripto* y su exención del IVA.

<sup>90</sup> Council Directive 2006/112/EC of 28 november 2006 on the common system of value added tax (OJ 2006 L 347, p.1, 'the VAT Directive').

<sup>91</sup> Los NFT pueden definirse como activos digitales únicos (no intercambiables) generados y mantenidos en esquemas de tecnología de registros de bloques.

Otra diferencia respecto a *bitcoin* es que, pese a que inicialmente se basaba en PoW, desde el 15 de septiembre de 2022 Ethereum se validó a través de PoS o cantidad de *ether* bloqueadas que tiene el validador y no en su fuerza computacional (Ethereum, 2021a, pp. 1-36). Este cambio, producido mediante un *hard fork*, se ha conocido como la fusión (*merge*) y ha permitido que Ethereum opere de una forma más ecológica, reduciendo notablemente la cantidad de energía requerida para validar un bloque (Mirza, 2022, pp. 1-6).

De esa manera, su generación y operativa se basa en un consumo energético más sostenible, evitando críticas y restricciones que se han abierto paso en las discusiones mantenidas en el seno de la UE dentro de MiCA que implementa novedades a este respecto. Entre ellas, la obligación de mostrar el impacto medioambiental de la tecnología aplicada en los libros blancos (art. 6.1. j, y 6.12 MiCA). Los criterios y metodologías se desarrollan vía normas técnicas de segundo nivel.

Por este motivo, el cambio de PoW a PoS en Ethereum se ve como generalmente positivo y sostenible, y permite el avance y desarrollo de soluciones en esta cadena de bloques de una forma más sostenible. Sin embargo, este cambio también implica un riesgo de concentración de nodos validadores en aquellos que acumulen mayor cantidad de *ether*, incrementando el riesgo de censura y reduciendo la característica de descentralización o democracia que la operativa descentralizada *Blockchain* quiere representar.

Finalmente, otra de las grandes ventajas que ofrece Ethereum es la posibilidad de transaccionar en *stablecoins*, cuyo concepto se desarrolla a continuación.

### ***2.3 Stablecoins o criptomonedas estables***

Las *stablecoins* son un tipo de criptoactivo cuya ventaja principal es estar referenciadas a un elemento de anclaje, que permite reducir la volatilidad de la que en general adolecen las criptomonedas (Bullman et al., 2019, pp. 1-55). Además, este tipo de monedas no dependen de los esquemas de pago, compensación y liquidación tradicionales (Panetta, 2020, pp. 1-5), por lo que están libres de los inconvenientes asociados a estos (costo, duración de la operación y falta de transparencia). En la actualidad, existen más de 200 criptomonedas estables emitidas o en desarrollo a nivel global (CBINSIGHTS, 2021, p. 6).



Debido a que reducen considerablemente el riesgo de alta volatilidad, se han planteado como una opción factible para realizar transferencias internacionales, que en la actualidad adolecen de ineficiencias en las infraestructuras de pago internacionales, altos costos y opacidad. De ser así, este tipo de criptoactivos podrían, en ciertos casos, llegar a un uso masivo (especialmente si son emitidas por los gigantes tecnológicos).

A este respecto, las *stablecoins* han ganado mayor popularidad a raíz de la frustrada propuesta realizada por un consorcio de grandes compañías tecnológicas, con el propio Facebook a la cabeza, de diseño de una criptomoneda estable propia referenciada a una cesta de monedas (Diem, anteriormente conocida como Libra) (Libra Association, 2020, pp. 1-29). Este proyecto levantó muchas opiniones por parte de las autoridades, puesto que podía suponer el nacimiento de una moneda digital privada estable, que además hubiese operado mundialmente y que hubiera sido considerada una moneda significativa, sistémica o global, engendrando una nueva dimensión de problemáticas legales, económicas, de supervisión y gestión de riesgos a las que hasta ahora los bancos centrales no se habían enfrentado.

En un escenario como el anteriormente descrito, este tipo de criptoactivos impactarían en el papel de los bancos centrales, sus políticas monetarias, de pagos y estabilidad financiera (Bailey, 2021, pp. 1-7). Además, podrían debilitar el papel de la banca comercial y, a largo plazo, provocaría una subida en los tipos de interés de los préstamos que ofreciera la banca tradicional (Bache, 2021, pp. 1-7), por lo que podría llegar a derivar la demanda de crédito hacia el mundo de financiación alternativa o parabancaria (Bailey, 2021, pp. 1-7).

El anclaje o mecanismo de estabilización puede ser de distintos tipos en función de la cercanía a modelos financieros ya conocidos (Bullman et al., 2019, pp. 1-55): referencia uno a uno a una moneda oficial, una combinación de monedas, activos del mundo real, de fuera de la cadena u *off chain* (por ejemplo, oro o inmuebles), o cestas de criptomonedas (*on-chain* o en la cadena). De referirse a monedas, la gran mayoría de *stablecoins* están referidas a dólares. Lo anterior se debe a que el bloqueo de cantidades masivas de euros en un escenario de tipos de interés negativos hacía que la moneda no fuera atractiva para mantenerla en depósitos con el fin de emitir criptomonedas estables referidas a euros.

Las *stablecoins* presentan un *trilema* entre la eficiencia del capital (esto es, el valor bloqueado en el mundo real), el tipo de colateral (divisas de curso legal o criptoactivos)

y el nivel de descentralización con respecto al colateral, siendo el caso más extremo las criptomonedas estables algorítmicas, que no cuentan con un colateral. Por tanto, tienen máxima eficiencia de capital y se basan en modelos puramente descentralizados (ver Figura 31).

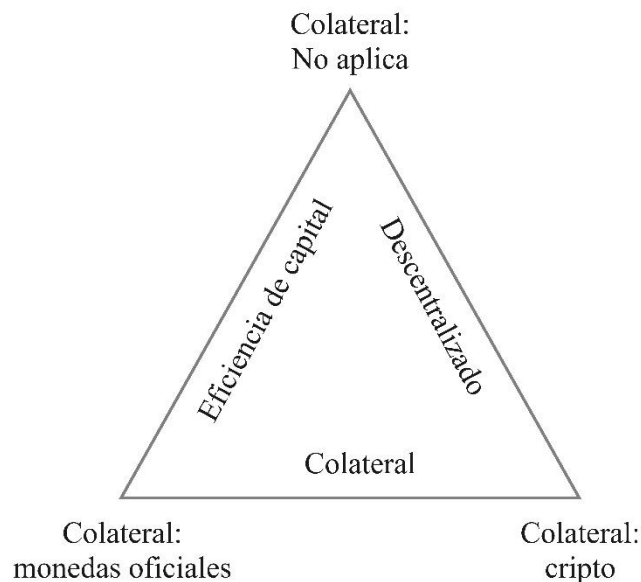


Figura 31. *Triángulo de las stablecoins*

Nota. Tomado de *Stablecoins: De-Risking Non-Collateralized Stablecoins*, por N. Wittayatanaseth, <https://medium.com/@natwittayatanaseth/https-medium-com-FinTech-kellogg-de-risking-non-collateralized-stablecoins-40e832562090>

El modelo más innovador y, por consiguiente, el más alejado de las realidades financieras existentes, es aquel cuya estabilidad está basada en algoritmos y no se rige o emite a través de ninguna institución en particular, de modo que no existe un responsable específico, siguiendo la tendencia de las DeFi. Sin embargo, las *stablecoin* algorítmicas no han tenido éxito y más bien han provocado altos niveles de desestabilización de los mercados cripto, especialmente en el caso de Terra-Luna en 2022. Cuando una *stablecoin* algorítmica generalmente aceptada en los mercados se “despegó” de su valor de referencia (en este caso, el dólar estadounidense), su cotización se desplomó.

Debido al amplio espectro de posibles diseños de las criptomonedas estables, su radio de operación (Financial Stability Board [FSB], 2020e, p. 10) y diseño de ecosistema a su alrededor, se hace necesario aplicar un enfoque flexible basado en riesgos, para poder acoger futuras evoluciones no contempladas o en desarrollo hoy en día.

En torno a la criptomoneda surge todo un ecosistema de actividades o negocios que en global se denominan los *stablecoin arrangements*. El *stablecoin arrangement* se define como “Un arreglo que combina una gama de funciones (y las actividades específicas relacionadas) para proporcionar un instrumento que pretende ser utilizado como medio de pago y / o depósito de valor”, incluyendo las reglas de gobernanza del arreglo, emisión y redención, la gestión de los activos, los servicios de custodia, la infraestructura, la provisión de transacciones, las billeteras, las casas de cambio, los ATM y los servicios auxiliares (Financial Stability Board [FSB], 2020c, p. 5).

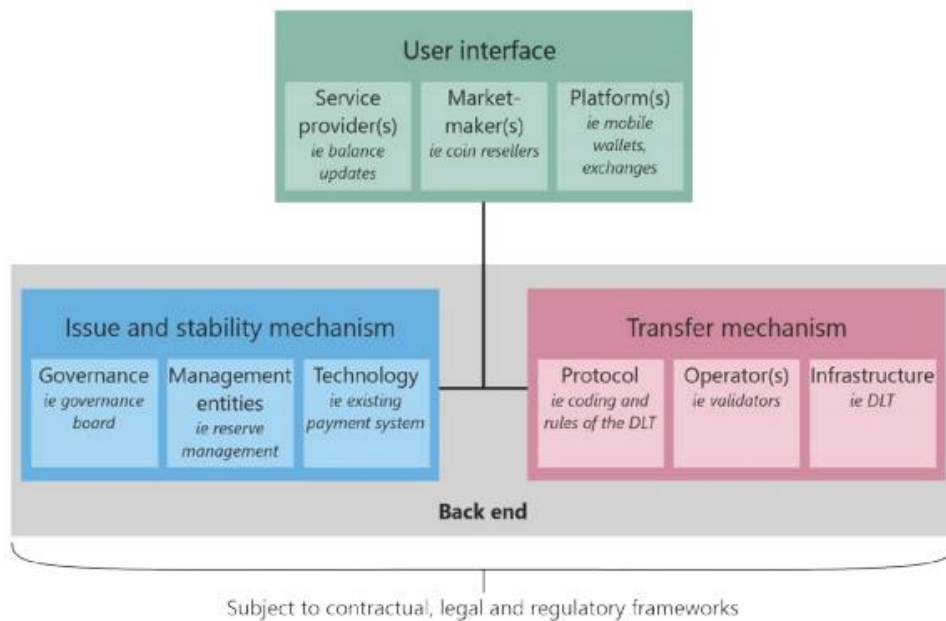


Figura 32. Visión funcional de un ecosistema stablecoin. Ejemplos seleccionados

Nota. Tomado de *Investigating the impact of global stablecoins*, por G7 Working Group on Stablecoins, 2019, <https://www.bis.org/cpmi/publ/d187.pdf>.

Respecto a sus potenciales casos de uso, cabe distinguir varios: desde el ángulo de situaciones con alta volatilidad, las *stablecoins* funcionan como valor refugio en casos de bajadas drásticas de criptomonedas no referenciadas como *bitcoin* o incluso de las propias monedas oficiales de determinados países como Venezuela o Argentina (Anderson, 2019, pp. 25-28).

Si se habla criptomonedas estables de uso global (globales, significativas o sistémicas<sup>92</sup>) (Bailey, 2021, pp. 1-7), en el supuesto de que estas contaran con una

<sup>92</sup> El artículo 39 del MiCA considera que los criterios para evaluar si una *stablecoin* es significativa o sistémica en función de su base de clientes, los accionistas del emisor, el valor de las *stablecoin* emitidas, su capitalización, el número y valor de operaciones, el volumen de reserva de activos, la importancia de sus actividades transfronterizas, la interconexión con el sistema financiero y el hecho de que la misma persona

adecuada gobernanza y confianza de los consumidores, podría contribuir a una mayor resiliencia en infraestructuras de pagos. Ello se debe a que cuentan con el potencial de poder convertirse en una alternativa válida de procesamiento de pagos (Segal-Knowles, 2021, pp. 1-7), especialmente internacionales a países en desarrollo, que es donde se detectan las mayores deficiencias en la actualidad. Esto potenciaría el uso de instrumentos de pago por parte de comunidades inmigrantes. Este tipo de público podría realizar pagos entre particulares (o *peer to peer*) sin necesidad de ningún tipo de intermediación, ahorrando costos y comisiones (CBINSIGHTS, 2021, pp. 20-21).

### 2.3.1 Control de las *stablecoins* sistémicas o globales: opciones de supervisión global

#### **a) Definición de criptomonedas estables significativas y criterios**

Una vez reconocido el potencial de este tipo de monedas, los bancos centrales han de evaluar cómo realizar una transición hacia estas nuevas realidades sin que se den incidentes graves que puedan provocar inestabilidad financiera o pérdida de confianza de la población (Segal-Knowles, 2021, pp. 1-7). El interés principal se encuentra en las llamadas *stablecoin* globales o sistémicas: criptoactivos de alto impacto debido a distintos factores como el volumen de operaciones, el número de clientes, los efectos de red, el volumen de ingresos o la extraterritorialidad. Las criptomonedas estables emitidas por grandes empresas tecnológicas entrarían dentro de esta categoría debido a que se desplegarían a nivel mundial y cuentan con un efecto de red sustantivo.

Además, en virtud del carácter global del diseño y operativa de estos criptoactivos, las barreras jurisdiccionales pierden peso (Bache, 2021, pp. 1-7), por lo que es necesario valorar posibles modelos de supervisión internacional. A continuación, se exponen tres posibilidades de gobernanza de autoridades en función del nivel de coordinación e integración entre países o regiones.

#### **b) Control local**

Este modelo se basa en la forma en la que operan actualmente los países respecto a los grandes conglomerados financieros. Cada país o región cuenta con sus propias reglas y existen acuerdos de colaboración e intercambio de información entre regiones o jurisdicciones, generalmente a través de *memorándums of understanding* bilaterales o

---

jurídica u otra empresa emita al menos una *token* con referencia a activos o *token* de dinero electrónico, y proporciona al menos un servicio de criptoactivos.

multilaterales (Financial Stability Board [FSB], 2020c, p. 21). Por lo general, se crearían agrupaciones de supervisores que compartieran posiciones o estrategias respecto a las *stablecoin (like-minded jurisdictions)* para permitir reconocimientos de entornos de control equivalentes (The CityUK, 2021, pp. 5-20).

Esta opción, sin embargo, corre el riesgo de quedarse limitada o no ser capaz de responder a tiempo, debido a que las *stablecoins* cuentan con una velocidad de transaccionalidad mucho mayor que las transacciones en efectivo o por medios de pago tradicionales (Long, 2021, p. 308). Además, diferencias de criterio podrían potenciar un arbitraje entre jurisdicciones y, por tanto, posibles movimientos de la moneda o entidades miembros del ecosistema hacia esas localizaciones.

En consecuencia, incluso este modelo necesitaría una modernización. Por este motivo, la formulación de una supervisión integrada (*embedded supervision*) (Auer, 2019, pp.1-31) que permitiera una colaboración y mejor entendimiento, especialmente entre las autoridades y el emisor de *stablecoins*, tanto en los diseños como en el control en tiempo real, sería una opción por implantar (Arner et al., 2020, pp. 1-31).

El uso, gestión y supervisión de estos nuevos modelos de negocio digitales parecen promover un cambio en el perfil del equipo supervisor, no solo en cuanto a las capacidades técnicas, sino también en cuanto a la mentalidad de apertura hacia la colaboración con el sector privado para un mejor entendimiento de sus modelos de negocios, riesgos y cómo gestionarlos (Comisión Europea, 2020c, p.1). Por esta razón, colectivos como el de los proveedores de servicios cripto de Estonia, proponen el desarrollo de unidades supervisoras *ad hoc* enfocadas en actividades de criptoactivos.

### **c) Supervisor de cabecera, supervisor de destino**

El modelo de supervisor de cabecera, supervisor de destino (*home state-host state supervisor*) seguiría el ejemplo de la propuesta de diseño que ha llevado a cabo la UE y que se ha aplicado hasta ahora en servicios financieros. Bajo este formato, existiría una autoridad competente en un país que lideraría el control sobre la criptomoneda estable (*lead overseer*) equivalente al supervisor de origen o supervisor de cabecera europeo y que concentraría el conocimiento de *stablecoin arrangement* (Financial Stability Board [FSB], 2020c, pp. 1-73). El resto de las jurisdicciones en las que operase, serían países de destino de los servicios.

Sin embargo, este modelo puede presentar problemas a la hora de su puesta en funcionamiento debido a varios aspectos. El primero es el hecho de que el ecosistema de la criptomoneda estable puede contar con distintas entidades en diferentes regiones (Financial Stability Board [FSB], 2020c, pp. 1-73), por lo que habría que fijar un criterio para considerar qué jurisdicción sería la de cabecera (si es donde se encuentra el órgano de toma de decisiones de gobernanza, la reserva o el diseño de la infraestructura). El segundo, que podría darse el supuesto de decisiones estratégicas de establecimiento en jurisdicciones con debilidades, bajos niveles de control o poca capacidad de supervisión de estructuras sistémicas. Por último, existen casos de criptomonedas estables descentralizadas en los que no hay una estructura de control o propiedad identificada, por lo que no es posible identificar qué jurisdicción sería la cabecera (Bailey, 2021, pp. 1-7; Financial Stability Board [FSB], 2020c, pp. 1-73).

#### **d) Coordinador de coordinadores**

Con el fin de superar las limitaciones indicadas anteriormente, el diseño de una autoridad de carácter internacional podría ser una opción por explorar. Entre las funciones principales de esta entidad estaría la fijación de estándares o guías de supervisión cripto con carácter holístico, la coordinación entre instituciones internacionales (IOSCO, Basilea o FATF) y la supervisión de *stablecoin arrangements* sistémicos en criterios de volúmenes mundiales o deslocalización de órganos decisores.

Este tipo de entidad diseñaría estándares o recomendaciones que se convertirían en estándares mínimos a nivel global y que serían puntos de partida para los desarrollos normativos a nivel regional o local. Bajo este modelo, podrían diseñarse plataformas de macro-supervisión de los mercados, con el objetivo de detectar señales de alerta y evitar inestabilidades globales, tales como fugas masivas de capitales o riesgos de falta de liquidez inminente. También podría ser capaz de asesorar el riesgo del total del ecosistema *stablecoin* y exigir refuerzos en las partes que conforman la cadena, ya sea en aspectos contractuales, de fraude o cualquier otro. De esa manera, el riesgo de la limitación en el asesoramiento integral de los riesgos por parte de los supervisores locales (G7 Working Group on Stablecoins, 2019, p. 5), se superaría a través de este punto común de concentración. Además, este tipo de autoridad podría ser una opción factible de supervisión de criptomonedas estables descentralizadas.

La tercera propuesta requiere mayor integración y podría plantear cuestiones de cesión de soberanía; sin embargo, debido al carácter global con las que ciertos *stablecoin arrangements* nacen, podría ser una solución comprensiva y eficaz.

### 2.3.2 Reflexiones

Las *stablecoins* parecen contar con un mayor potencial de adopción masiva con una estructura de gobernanza adecuada que permita obtener la confianza tanto del público como de los organismos supervisores. Para ello, se debe diseñar un plan de gestión del cambio ordenado con el fin de mitigar el impacto que estas nuevas monedas puedan tener en la estabilidad financiera. Como indicó Segal-Knowles (2021):

[...]no ha de confundirse con la preservación del status quo. La estabilidad financiera no se trata de proteger a los bancos establecidos u otras empresas existentes de la competencia. [...]la estabilidad financiera busca garantizar que las personas y las empresas puedan confiar en los servicios financieros esenciales, [...]tanto en los malos como en los buenos tiempos. (p. 1-7)

Será requerirá un desarrollo de marcos normativos y *soft law* a lo largo de los próximos años que establezcan los parámetros para un adecuado cumplimiento de los *stablecoin arrangements*. Si bien es cierto que ya existen organismos emitiendo guías, como FATF, será necesario ver cómo estas encajan en la operativa real de este tipo de actividades y si debe ampliarse el foco (por ejemplo, FATF se ha centrado en recomendaciones a proveedores de servicios de pagos, custodios y cambio, no tanto a emisores o sistemas de gobernanza) (Financial Stability Board [FSB], 2020c, pp. 14-16). El enfoque tomado hasta la fecha es el de asimilar el ecosistema de las *stablecoins* a los modelos ya conocidos, pudiendo resultar oneroso para jugadores de menor tamaño. Además, estos requerimientos implican costos añadidos que probablemente se trasladarán al público en general.

Respecto a los modelos de supervisión, es posible que sea necesaria una mayor integración y coordinación a nivel global, con el propósito de evitar riesgos sistémicos a través de una nueva figura de autoridad cripto que pueda fijar criterios globales y supervisar las criptomonedas estables significativas o sistémicas de una forma macro. A su vez, debido al nuevo planteamiento tanto de las finanzas como de la interacción con los supervisores, será necesaria la apertura al diálogo público-privado. En ese sentido, herramientas como la supervisión integrada, monitorizaciones en tiempo real y el diseño

de unidades de supervisión especializadas (Comisión Europea, 2020c, p.1), con conocimientos técnicos y apertura al cambio, serán necesarios a lo largo de los próximos años.

### **3. Criptoactivos de emisión pública: monedas digitales de bancos centrales<sup>93</sup>**

#### ***3.1 Introducción***

En octubre de 2020, el BCE publicó su informe titulado *Report on a digital euro* (European Central Bank [ECB], 2020b, pp. 1-55), sometiéndolo a consulta hasta enero de 2021. Tan solo la cifra de respuestas (8221) pone de manifiesto el interés generado por esta iniciativa en el mundo financiero y el público en general (European Central Bank [ECB], 2021b, p.1).

La decisión europea tiene su origen en las discusiones sobre la posibilidad de creación de monedas digitales de bancos centrales. El asunto se estaba evaluando en el seno del BIS, como organismo coordinador de bancos centrales en asuntos relacionados con pagos, compensación y liquidación desde 2018 (Cœuré, 2018, pp. 1-5). Debido a ello, cabe plantearse cuál es el motivo de que en la zona euro se haya optado por impulsar este proyecto ahora, pasando de una posición inicialmente negativa<sup>94</sup> (Wald & Rochemont, 2019, pp. 1-52), hacia el estado actual, y qué implicaciones pueden tener en contextos regulatorios y de supervisión.

El presente apartado aborda la aparición de las criptomonedas estables como uno de los elementos clave de respuesta a este interrogante. También propone la situación geopolítica como un segundo motivo de impulso a este nuevo tipo de monedas. Con el fin de enmarcar la discusión, se expone el concepto de CBDC en contraposición a las *stablecoins*, identificando cuáles son sus casos de uso, ventajas e inconvenientes. Para ello, se analizan principalmente los informes emitidos por el BIS y el BCE entre 2018 y 2021.

---

<sup>93</sup> Esta sección es un extracto de *Central Bank Digital Currencies (CBDC): reacciones de los bancos centrales ante la expansión del uso de criptomonedas y sus implicaciones jurídico-económicas*". Suárez, L. (2022). Central Bank Digital Currencies (CBDC): Reacciones de los bancos centrales ante la expansión del uso de criptomonedas y sus implicaciones jurídico-económicas. En Parra, C., *Derecho digital y nuevas tecnologías* (pp.937-956). Aranzadi. España.

<sup>94</sup> El 14 de septiembre de 2018, Reuters publicó una noticia en la que se expuso que Mario Draghi había afirmado que "*The ECB and the Eurosystem currently have no plans to issue a central bank digital currency*" (Reuters, 2018, p. 1).



Posteriormente, se examinan los presupuestos de la aparición de las CBDC como reacción ante la amenaza de las *stablecoins*, así como su relación con elementos geopolíticos. Finalmente, se plantean problemáticas de política pública y diseño de la propia moneda central si se busca neutralizar o desincentivar el uso de criptomonedas estables.

### **3.2 Estado de la cuestión**

Europa ha desarrollado principalmente dos iniciativas relacionadas con criptoactivos y CBDC. La primera de ellas fue la propuesta del reglamento relativo a los mercados de criptoactivos del 24 de septiembre de 2020 (MiCA)<sup>95</sup>, que ha sido publicado el 9 de Junio de 2023, bajo la denominación de Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, y que forma parte de la estrategia de finanzas digitales para la UE<sup>96</sup>. La segunda gran iniciativa en esta temática es el mencionado informe sobre el euro digital emitido por el BCE, donde se idea el lanzamiento de una moneda digital emitida por esta autoridad.

De este modo, la UE dio pasos significativos al reconocer el potencial de los criptoactivos y su necesidad de diseño de los esquemas regulatorios adecuados. Además, el propio BCE entró en la carrera por el diseño de su propio CBDC, afrontando el reto de qué tipo de ámbito y diseño será el más adecuado para la región.

En concreto, MiCA reconoce la continua evolución que están experimentando los criptoactivos, subrayando especialmente el impacto de las criptomonedas estables, puesto que podrían llegar a ser “generalmente aceptadas y potencialmente sistémicas”. El principal foco de impacto reside en las criptomonedas estables significativas, también llamadas sistémicas o globales.

En ese orden de ideas, parece existir una cierta relación de competitividad entre este tipo de criptomonedas y las CBDC, como herramienta de respuesta de bancos centrales.

---

<sup>95</sup> Unión Europea. Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva UE 2019/1937 del 24 de septiembre de 2020. COM/2020/593 final. 2020/0265 (COD).

<sup>96</sup> Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Estrategia de Finanzas Digitales para la UE, COM (2020) 591, del 23 de septiembre de 2020.

Sin embargo, el éxito de esta réplica dependerá en buena medida del tipo de CBDC que se diseñe, las limitaciones que se impongan, su finalidad y los casos de uso autorizados.

### **3.3 CBDC: concepto, tipos y finalidad**

El BIS definió las CBDC como “potencialmente una nueva forma de dinero digital del banco central que se puede distinguir de las reservas o saldos de liquidación mantenidos por bancos comerciales en bancos centrales” (Bank of International Settlements, 2018, p. 1). Las CBDC son emitidas por bancos centrales y, por tanto, respaldadas o garantizadas por estos (Barrio, 2021).

Este tipo de monedas se caracterizan por ser electrónicas, emitidas por bancos centrales y cuentan con la posibilidad de realizar operaciones entre iguales o *peer to peer*<sup>97</sup>. Dependiendo de la finalidad de su diseño y sus características, podrían ser utilizadas por el público en general (también llamadas *retail* CBDC) o restringidas a grandes corporaciones (las denominadas mayoristas o *wholesale* CBDC) (Bech & Garrat, 2017, pp. 1-16).

En función del tipo de tecnología aplicada para su diseño, se clasificarían como *tokenizado* o basado en el modelo de cuentas. Cualquiera de las dos opciones, abre una serie de preguntas que deberán resolverse a lo largo de los próximos años. A modo de ejemplo, el optar por un estándar *tokenizado* plantea cuestiones sobre una posible reducción de balances en cuentas comerciales a favor de fichas de carácter público (CBDC). Por su lado, un modelo basado en cuenta implicaría la apertura de cuentas del público general en el banco central, impactando o cambiando el rol de los bancos comerciales, pero limitaría la anonimidad con la que se opera hoy en día con el efectivo.

Por este motivo, dentro del proyecto del euro digital el BCE está evaluando limitar el valor en estas cuentas centrales a 3000 euros o imponer intereses a partir de una determinada cantidad (Bartz, 2021, pp. 1-3). Como se puede observar, el proyecto de emisión de una CBDC implica un gran esfuerzo en términos de tiempo y recursos. De esta forma, se debe plantear cuáles son los casos de uso, sus ventajas y riesgos, y por qué en la actualidad los bancos centrales se han embarcado en este tipo de iniciativas.

---

<sup>97</sup> Estas características se identificaron de manera gráfica en la llamada “flor del dinero” (Bech y Garrat, 2017, p. 1).

### 3.4 Casos de uso, ventajas y riesgos de las CBDC

#### 3.4.1 Casos de uso

Dependiendo del tipo de moneda digital del banco central que se esté diseñando por el país, cabe identificar las distintas razones de origen y, por tanto, los casos de uso. Si se toma como ejemplo la e-Krona sueca (Sveriges Riksbank, 2021, pp. 1-21), el banco central sueco busca eliminar el riesgo de exclusión financiera en el país, derivado de la reducción del uso de efectivo y el aumento de las transacciones electrónicas. Por este motivo, el diseño de su CBDC es de *token* para público en general.

Respecto a la utilidad de CBDC *wholesale*, estarían enfocados en países con infraestructuras de pago inmaduras, fragmentadas o poco desarrolladas. Una potencial moneda con estas características permitiría la mejora en tiempo, costo y eficiencia de pagos domésticos. Sin embargo, para entornos como el europeo, que cuenta con sistemas de pago instantáneos (TARGET 2), no presenta un salto cualitativo tan material como en otras regiones (Deloitte tax and consulting Sarl, 2020, pp. 1-26).

#### 3.4.2 Ventajas

Las ventajas que ofrece una potencial CBDC pueden analizarse desde dos perspectivas: desde la óptica del sistema macroeconómico y desde el plano del público general.

Desde el punto de vista de los sistemas e infraestructuras globales, un modelo de CBDC basado en cuentas en bancos centrales reduciría saldos en bancos comerciales, por lo que potencialmente reduciría los depósitos bancarios (Ordóñez, 2021, p. 1-6) y, por consiguiente, los riesgos de “*too big to fail*”. Por esta razón, podría potencialmente ayudar a reducir la carga de supervisión y control que existe en la actualidad hacia la banca comercial. Un caso así permitiría la reducción de barreras de entrada al sector financiero (Ordóñez, 2021, p.1-6) y una disminución del nivel de proteccionismo con el que cuenta la banca comercial actualmente (Awrey, 2021, pp. 1-70). Las políticas monetarias de los países se harían más efectivas, debido a que se reduciría el efecto distorsionador de la emisión de dinero privado por parte de los bancos comerciales.

En el caso europeo, un euro digital ayudaría a conseguir una unión monetaria real. Al respecto, M. Fernández Ordoñez afirmó:

*No es lo mismo un depósito en un banco alemán u holandés que en un banco griego, español o italiano. En caso de crisis, la solidez de los euros digitales depende de la solidez de las haciendas nacionales y el aseguramiento de esos euros es diferente según los países.* (Ordóñez, 2021, pp. 1-6)

Para las propias instituciones supondría la reducción de costes en términos de esfuerzo de impresión de dinero físico y distribución de este, si se tiene en cuenta que, pese a que el euro digital no pretende eliminar el dinero físico, la realidad es que el uso de dinero físico está decreciendo en pro de las transacciones electrónicas. Esta situación se acentuó tras la crisis de la COVID-19.

Respecto al público en general, las CBDC supondrían una mejora en seguridad en los pagos, eficiencia (Deloitte tax and consulting Sarl, 2020, pp. 1-26) y reducción de costos en las operaciones (Barrio, 2021). El potencial de obtener un dinero programado permitiría gestionar niveles de anonimato adecuados o controles relacionados con las sanciones financieras internacionales, contrarrestando los riesgos actuales en términos de privacidad y crimen financiero.

Desde el punto de vista del usuario, contaría con una moneda digital de menor volatilidad que las criptomonedas, estaría garantizado y, bajo la premisa de ser *tokenizada*, probablemente no tendría el riesgo de pérdida de claves de acceso que tienen en la actualidad las monedas como *bitcoin* o *ether*. Además, al no ser emitidas por instituciones privadas, no existirían dudas sobre el posible uso de los datos con fines comerciales o la gestión de estos en países terceros no equivalentes.

### 3.4.3 Riesgos

El principal riesgo que presentan las CBDC es el de provocar una huida del dinero físico o *fiat* hacia este nuevo tipo de moneda. Una CBDC sin limitaciones provocaría una reestructuración fundamental del sistema financiero, debido a que, como se indicó anteriormente, conllevaría una reducción de los depósitos en los bancos comerciales (Guaita et al., 2019, pp. 5-160) y una disminución de las barreras del sector, consiguiendo un escenario de mejora de niveles de competencia (Ordóñez, 2021, pp. 1-6). Por este motivo, Europa proyecta establecer límites con el fin de controlar su impacto.

Pese a la limitación planteada por el BCE, la reducción en los depósitos de bancos comerciales europeos podría estimarse en unos 873 billones de euros, lo que se estima en

una reducción media de un 8 % de los depósitos de la zona euro, siendo los bancos en países de menor tamaño los más perjudicados según Morgan Stanley (Jones, 2021, pp. 1-2). En otro plano, esta nueva modalidad de monedas lleva en sí riesgos distintos a los de la emisión de monedas físicas, principalmente de ciberseguridad. Los riesgos clásicos de falsificación se trasladan al mundo digital mediante potenciales manipulaciones criptográficas.

### **3.5 ¿Por qué CBDC ahora? Geopolítica, finanzas y criptoactivos**

#### **3.5.1 Factores geopolíticos y financieros**

Si se toman en cuenta las iniciativas en los Estados más avanzados (lanzadas, en desarrollo o con pilotos de testeo), se evidencia que en la UE tan solo Francia, Ucrania y Suecia han alcanzado este nivel de progreso. La gran mayoría de los casos en mayor madurez pertenecen a países emergentes, en los que el nivel de aceptación e interés es mayor debido a que los niveles de bancarización de la población son menores (Conesa, 2021).

Respecto al panorama total de proyectos, el BIS ha identificado un aumento de estos a lo largo de los últimos años (Boar y Wehrli, 2021, p. 11). Factores como la geoestrategia política de los países no pueden dejar de considerarse en estos casos, especialmente si se habla del yuan digital. El estado avanzado de esta CBDC ha permitido realizar pruebas de concepto en Shenzhen para pagos diarios, tales como servicios de taxi y restaurantes a domicilio (John, 2020, pp. 1-4). Además, ha anunciado su siguiente paso con tests con Hong Kong y Macao, así como la colaboración con el Bank of Thailand y el Bank of UAE para operativas transnacionales (Caudevilla, 2021a, p. 1-2). El lanzamiento temprano al mercado de una CBDC por parte de una de las grandes potencias supone una ventaja en términos de adopción de esta moneda en el comercio internacional (Caudevilla, 2021b).

Los escenarios anteriormente indicados no se dan en la zona europea, dado que se opera dentro de un entorno de pagos consolidado y la brecha de inclusión financiera es menor; sin embargo, el factor geopolítico también podría aplicar a este caso, dado que la adopción del yuan digital tendría un impacto en el comercio exterior europeo. Asimismo, cabe plantearse si la amenaza de una *stablecoin* global ha sido otro de los factores desencadenante del impulso al proyecto del euro digital (European Central Bank [ECB],

2020b, p. 11). Se trataría, similar al caso del yuan, de una entidad con gran potencial de adopción temprana por parte del público, pudiendo minar la soberanía de la zona en lo que respecta a políticas monetarias.

### 3.5.2 Criptoactivos: la competencia de las *stablecoins* globales

Las global *stablecoins*, en concreto Diem, fueron calificadas por Cecilia Skingsley como una “llamada de atención” a los bancos centrales para que busquen nuevas soluciones en entornos de pagos (Bank of International Settlements [BIS], 2021b).

La estrategia de Diem era la emisión de varios tipos de criptomonedas estables por parte del mismo consorcio: habría aquellas emitidas contra una moneda local (euro, dólar, entre otros) que se denominan *single-currency stablecoins*, y tendrían como garantía depósitos y bonos a corto plazo del gobierno correspondiente (Sandner et al., 2020, pp. 2-27). Por otro lado, se proponía una cesta de las *single-currency stablecoins* para la emisión de una *multi-currency stablecoin*, que era conocida por el público como Libra (LBR) y que posteriormente pasó a denominarse Diem (Sandner et al., 2020, pp. 2-27). Por este motivo, el impacto era doble en el mercado europeo a través de su *single-currency stablecoin* basada en euros, y mediante su *multi-currency stablecoin* basada en una cesta que contenía el euro y que podría operar de manera global.

Como se mencionó anteriormente, se trata de monedas digitales de emisión privada que pueden estar referenciadas a una moneda, cesta de monedas, valores o activos tales como oro o petróleo, entre otros (Mohanti, 2019, pp. 1-180).

Este tipo de criptodivisas suponen una amenaza para los bancos centrales por varios motivos: las criptomonedas estables significativas o globales serían emitidas por grandes corporaciones que operan a nivel mundial. Esto hace que partan de una importante masa crítica de clientes, que en el escenario de grandes tecnológicas como Facebook hubiera sido mayor que muchos de los bancos que operan hoy en día a nivel internacional, y su nivel de penetración hubiera sido mayor en aquellos países de mayores brechas entre la población que cuente con una cuenta Facebook versus una población bancarizada (Eichler y Thum, 2019, p. 21).

Dado que son monedas de emisión privada, los bancos centrales verían mermada su capacidad de influencia sobre la política monetaria de los países. Un emisor privado en países con bajos niveles de bancarización podría llegar a convertirse, *de facto*, en una

especie de competidor de los propios bancos centrales en términos de política monetaria (Groß et al., 2019, pp. 1-7). Las políticas expansivas de los bancos centrales, bajo este tipo de escenarios, tendrían un menor efecto, alterando así la capacidad de ajuste de la inflación en los países.

Desde el punto de vista de los bancos comerciales, un Diem hubiera implicado que la asociación Libra hubiese tenido que colateralizar altas sumas de moneda de curso legal correspondiente para su emisión (similar a las entidades de dinero electrónico), provocando problemas de liquidez<sup>98</sup> en la banca (Klein, 2021, pp. 1-23) y, a su vez, los depósitos de sus usuarios migrarían de la banca comercial hacia el formato criptomoneda estable. A estas preocupaciones se añaden las relativas a la protección de datos y uso de estos o de cómo se articularía la supervisión de una criptomoneda estable de tipo significativo, que presenta desafíos regulatorios aún por identificar.

### ***3.6 Retos jurídico-económicos para los bancos centrales***

Frente a este nuevo escenario, los bancos centrales tienen varios retos jurídicos que plantearse y que en la actualidad se encuentran en fase de discusión. A continuación, se indican los principales.

En primer lugar, se encuentran las limitaciones al euro digital. Como se argumentó anteriormente, debido a que se busca una convivencia del euro digital con el entorno de producción monetaria actual, se ha planteado limitar el euro digital (Conesa, 2021). Sin embargo, estos casos restarían atractivo a la moneda (Bofinger, 2021) y podrían incentivar indirectamente el uso de *stablecoins*, que no cuentan con las limitaciones antes mencionadas y, por tanto, no evitaría la erosión en el impacto de las políticas monetarias.

Un euro digital sin limitaciones podría reducir los niveles de protección que el sector financiero tiene en la actualidad, pero provocaría inestabilidad en el sistema financiero. Bajo el escenario del euro digital no limitado, el banco central perdería poder, dado que su rol es la pura emisión de las CBDC, deslindando la emisión de monedas digitales de su distribución. (Awrey, 2021, pp. 1-70)

Un segundo reto se presenta en términos de anonimato versus prevención del crimen financiero: una de las grandes preguntas es cómo encontrar un balance entre el anonimato

---

<sup>98</sup> Caitlin Long indicó que el BCE estimó en mayo de 2020 que en el caso de Facebook se podría crear un silo de liquidez de unos tres trillones de dólares (Long, 2021, pp. 307-319).

o no control gubernamental (principal atractivo del efectivo y de los criptoactivos) frente a la necesidad de controlar la moneda para evitar su uso con fines ilícitos. Actualmente, buscan soluciones para enmascarar los datos o programar el dinero contra listas de sancionados, pero se enfocan en alcanzar un alto nivel de privacidad, no el anonimato total (Conesa, 2021). Por otro lado, la falta de herramientas por parte de las instituciones privadas para controlar los movimientos de criptoactivos llevan al rechazo de este tipo de negocios, que suelen terminar en litigio<sup>99</sup> (véase el recurso de apelación AP Asturias, sec. 4ª, S 06-02-2015, n.º 37/2015, rec. 27/2015) debido a que pueden considerarse como fórmulas encubiertas de discriminación hacia el sector cripto.

En la actualidad, se buscan soluciones que equilibren la privacidad y los deberes relacionados con el crimen financiero. A modo de ejemplo, el Sand Dollar de Bahamas emplea tecnología de IBM (Fabric) con el fin de asegurar adecuados niveles de cumplimiento y privacidad (Bison Trails, 2021, p. 16).

Finalmente, existe la necesidad de revisar la regulación para incluir este nuevo medio de pago, puesto que queda por decidir si estas nuevas monedas se limitarán también en su uso o si podrán ser equivalentes al dinero físico, en cuyo caso se haría necesaria una revisión general de los contextos normativos locales para la aceptación de este tipo de monedas como medio de pago o instrumento de inversión. La distinción entre monedas de uso general y monedas de uso mayorista abre el argumento sobre la necesidad de distinción de estas en la regulación, indicando a qué tipo de operativas se limitarían cada una de ellas (Schwarcz, 2021, pp. 1-51).

### ***3.7 Categorías de controversia: non fungible token (NFT o token no fungible)***

Los NFT se encuentran a caballo entre el mundo financiero y el no financiero (por ejemplo, el arte o la música). Han sido uno de los grandes protagonistas del panorama cripto desde 2020 (Bao y Roubaud, 2021, pp. 44-46), adquiriendo una verdadera relevancia a raíz de la explosión de su mercado en 2021. Incluso se han llegado a considerar como la siguiente iteración de la tecnología *Blockchain* (Fairfield, 2022, pp. 1261-1314) y la puerta de entrada hacia los mundos de realidad virtual que se encuentran en el metaverso<sup>100</sup>.

---

<sup>99</sup> Recurso de Apelación AP Asturias, sec. 4ª, S 06-02-2015, n.º 37/2015, rec. 27/2015, 2015.

<sup>100</sup> El metaverso son mundos de realidad virtual donde los usuarios pueden realizar actividades que replican la vida real a través de sus representaciones (avatares). Como tales, cuentan con sus propios negocios,



Los NFT se pueden definir como un “criptoactivo único que representa derechos sobre un subyacente activo ‘*tokenizado*’, a menudo digital, que se crea y transfiere usando DLT” (Clifford Chance, 2021, p. 3). Estos *tokens* pueden considerarse como equivalentes a una escritura o certificado de propiedad, es decir, que son datos en la cadena de bloques que representan algo que puede estar contenido en esta o no, material (inmueble) o no (se han llegado a vender NFT de sentimientos). Por este motivo, se juzga que los NFT tienen dos componentes: el subyacente (*NFT ítem*) y el *token* en *Blockchain* (*NFT metadata*<sup>101</sup>) que contiene detalle de la propiedad, la transacción, el objeto de la transacción y su localización (Busch, 2022, p. 2).

Por lo general, se pueden identificar ciertas características propias e inherentes de los NFT (Martinero, 2022, pp. 329-357). Primero, representan un certificado de autenticidad mediante el empleo de DLT, siendo su piedra angular el desarrollo de los contratos inteligentes, sin los cuales los NFT no existirían. Segundo, no son fungibles (esto es, no intercambiables) y cuentan con un sello de tiempo. Además, son verificables y no cabe posibilidad de falsificación de estos. Tercero, no requieren de un tercero de confianza que valide o verifique. Finalmente, existe una cuarta característica que tradicionalmente se ha tenido en cuenta y que Martinero Tor identificó como la ausencia de posibilidad de fraccionamiento en distintas partes, que ha devenido no válida en el tiempo, puesto que en la actualidad existe la posibilidad de fraccionamiento de NFT.

La naturaleza legal y, por tanto, el nivel de protección de los NFT no queda clara debido a la falta de un esquema legal que dote a la figura de ciertos niveles de seguridad jurídica. Esto origina serios problemas de indefensión por parte de los artistas y propietarios. A este respecto, el 29 de abril de 2022, The Art Newspaper publicó un artículo en el que informó que, por primera vez en el mundo, la corte inglesa reconocía los NFT en sí como una propiedad con capacidad de tener protección legal, permitiendo la emisión de órdenes judiciales a las plataformas de compraventa de NFT para congelarlos y obtener información de los dueños de las direcciones DLT que hubieran incumplido derechos de propiedad intelectual o autoría (Pryor, 2022, pp. 1-3).

---

gobernanza y finanzas. Las DAO o DApps son propios de estos nuevos mundos. En el metaverso, la economía se basa en *tokens*, motivo por el cual los *tokens* de gobernanza, criptodivisas y NFT se consideran como las monedas necesarias para operar dentro de estas realidades (Vidal-Tomás, 2022, p. 102742).

<sup>101</sup> Los metadatos (*metadata*) son aquellos datos que describen o hacen referencia a otros (por ejemplo, describen el tipo de archivo, el contenido, la fecha de creación, la modificación, entre otros).

En España, la interpretación jurídica de los NFT y las plataformas de compraventa de estos se ha llevado a cabo en el ámbito fiscal mediante la resolución de la DGT al dar respuesta a la Consulta Vinculante V0486-22 el 10 de marzo de 2022. En dicha resolución se aclara que la venta de NFT no puede identificarse como entrega de bienes debido a la ausencia de la entrega física del archivo digital (lo que se vende es el NFT en sí, no la obra subyacente). En ese sentido, se hablaría de una prestación de servicios, en la que por lo general se vende a contrapartes particulares (no empresarios), y que estaría sujeta a IVA del 21 %. Este enfoque no aseguraría un *level playing field*, dado que las obras de arte están sujetas a un IVA del 10 %, causando así un agravio con base en la tecnología subyacente.

Por otro lado, desde el punto de vista tecnológico, los NFT se asociaron inicialmente con un tipo de ERC determinado (el ERC 721). Sin embargo, las nuevas estructuras han ido apareciendo, entre las que se incluyen los ERC 1155, que tienen capacidad de representación tanto de *tokens* fungibles como no fungibles; los ERC 994, que representan bienes inmuebles; y los ERC 989, que representan la relación con otro *token* (Moreno, 2021, p. 70-71).

Respecto a su taxonomía, existen diversos criterios de clasificación que podrían aplicarse: (i) según el elemento representado, (ii) su capacidad de fraccionamiento, (iii) los derechos otorgados, (iv) según el rol del creador/emisor y (v) según el contexto. La clasificación en función del elemento representado podría considerarse un formato en árbol, en el que la principal rama sería si el NFT se concibe como un componente en la cadena (*on chain*) o un elemento fuera de la cadena (*off chain*).

Los NFT que representan elementos en la cadena consisten en casos en los que el propio NFT representa un elemento digital que está contenido en la cadena de bloques y que es “*hasheado*” directamente en la ficha. Estas circunstancias solo se dan si, por ejemplo, la obra de arte requiere de una capacidad de almacenaje reducida. La gran ventaja de este tipo de NFT es la independencia, en el sentido de que la obra de arte no desaparecería, como podría suceder si se referencia a elementos físicos o incluso virtuales (por ejemplo, se perdería una obra de arte fuera de la cadena de bloques si el servidor que la hospeda se cierra).

Los NFT que representan elementos *off chain* son aquellos que apuntan hacia un elemento que no se encuentra en la cadena de bloques. Aquí cabría una subdivisión entre NFT que representan elementos ajenos a la *Blockchain* como bienes materiales (bienes

muebles o inmuebles) o inmateriales (por ejemplo, marcas o patentes), derechos o incluso obligaciones (Moreno, 2021, p. 70-71).

Esta distinción es clave, puesto que, en los casos de representaciones fuera de la cadena, el NFT simplemente funciona como un registro de quién es propietario o propietaria del artículo, pero este no está contenido en la ficha, sino en otro espacio (ya sea físico o digital, como una web o un servidor). En este caso, parte de los metadatos del NFT incluirán una especie de referencia que apunta que esa ficha está vinculado a un elemento (similar a cuando en la escritura de compraventa de un inmueble se indica la dirección de dónde está ubicado este).

Debido a esta separación entre el título (NFT) y el elemento que este representa (por ejemplo, un inmueble o una página web), el subyacente no tiene las mismas garantías de inmutabilidad que el NFT, pudiendo sufrir alteraciones, fraudes, robos o incluso eliminaciones. En este último caso (eliminación), el NFT dejaría de tener valor, dado que el subyacente se perdería o destruiría.

El segundo tipo de clasificación en función de su capacidad de fraccionamiento es precisamente uno de los puntos que llevan hacia el debate de si los NFT deben regularse bajo la normativa financiera o no. Pese a que se pueda entender que los NFT, como elementos no fungibles y únicos, no pueden intercambiarse, en realidad, existe la capacidad de diseño de dos tipos diferentes de NFT: aquellos que son un elemento simple e indisoluble (el concepto común de NFT) y aquellos en los que se establece la posibilidad de fraccionamiento en su programación. En este último caso, cada una de las direcciones que compren serían propietarias de una fracción del NFT. Son precisamente estos casos los que generan dudas sobre si podrían considerarse instrumentos financieros bajo MiFID II.

La tercera clasificación que se puede observar es aquella relativa a los derechos otorgados por la adquisición del NFT. Esto se debe a que puede haber NFT libres de restricciones, pero también pueden existir NFT en los que se establecen condiciones específicas que limitan los derechos de uso y gestión de estos por parte de sus adquirentes. A modo de ejemplo, se pueden establecer limitaciones como la de prohibir los *Marketplace* para realizar la compraventa de las fichas no fungibles, el uso de estos en webs, los eventos de promoción o publicidad e incluso el que el dueño los use como asociados a su imagen (Fairfield, 2022, p. 1284). En ese sentido, los metadatos del NFT no representan necesariamente la propiedad legal sobre el subyacente, ni mucho menos

transfieren derechos de propiedad intelectual o autoría sobre el subyacente (material o digital) (Busch, 2022, p. 2).

La anterior clasificación deja ver que el creador del NFT puede establecer condiciones o criterios en el NFT que, de alguna forma, lo relacionan con su originador pese a las sucesivas transmisiones de propiedad que pueda experimentar (Fairfield, 2022, p. 1284). Esto hace deducir la existencia de una cuarta clasificación en función del rol de este originador o emisor. Pueden darse casos en los que hay un completo desapego tras la primera operación de emisión y venta del NFT (este caso puede catalogarse como un NFT libre). Sin embargo, cabe la posibilidad de que el emisor se reserve la propiedad sobre el NFT (por ejemplo, en un NFT fraccionado, que el creador mantenga ciertas fracciones de este en propiedad) o incluso que programe vía *smart contract* el pago automático de un porcentaje del valor de cada compraventa que suceda en el futuro (Fairfield, 2022, p. 1284).

Finalmente, los NFT pueden depender o no de un contexto (Fairfield, 2022, p. 1284). Un NFT que represente una obra de arte podría considerarse como independiente en este aspecto, puesto que su valor depende de la obra en sí y las apreciaciones que se den de ella en el futuro. Sin embargo, existen NFT que tienen una gran dependencia del contexto en el que se generan y, por tanto, de los “dueños” de dicho contexto. A este respecto, Fairfield mostró un claro ejemplo: cualquier NFT que represente una característica dentro de un juego (por ejemplo, una piel, una herramienta). En este caso, el valor viene dado por aspectos como, por ejemplo, si es empleable en otros juegos (interoperabilidad) o si es raro en un juego muy conocido (escasez). No obstante, si los dueños del juego decidieran desmantelarlo, el valor del NFT se perdería.

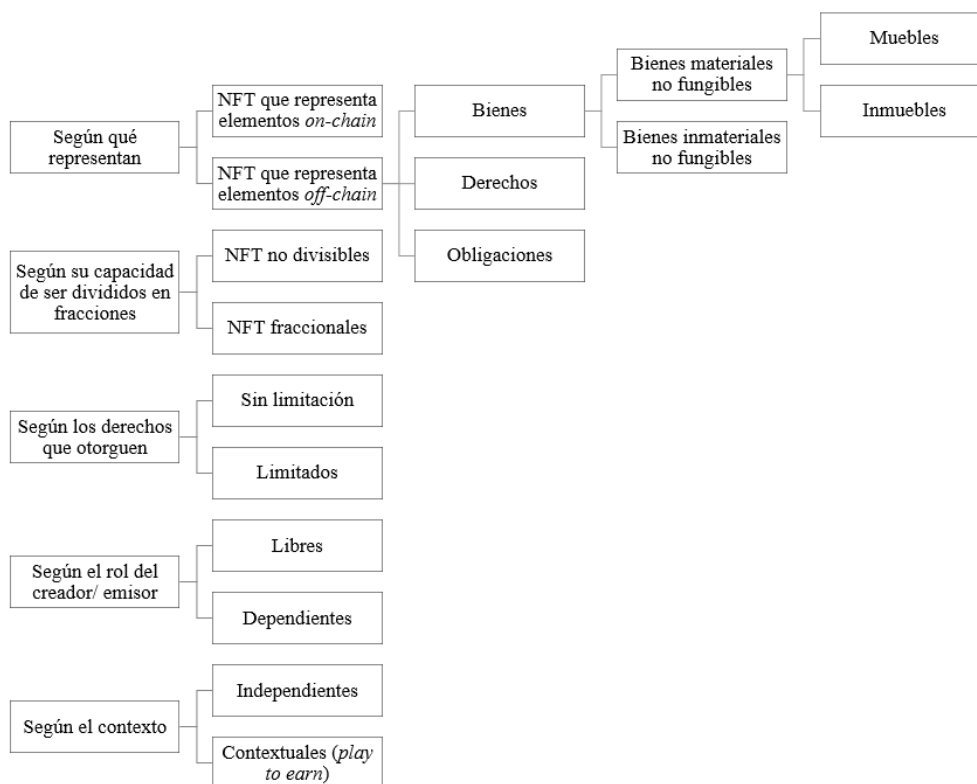


Figura 33. Taxonomía de tokens no fungibles (NFT)

Fuente: elaboración propia.

Los NFT abren muchos tipos de debates legales, especialmente en el mundo financiero, y suscitan el debate de si deben estar regulados y bajo qué normativas, en caso de serlo. Desde el punto de vista de blanqueo, la quinta y sexta directivas aplican una definición amplia de activos virtuales (definición empleada por estas directivas, no por el proyecto del MiCA) como la siguiente:

*Representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.* ((18) de la Directiva (UE) 2015/849 incorporado vía Directiva (UE) 2018/843, art. 3)

Si bien la definición es amplia, la consideración de que los activos virtuales deben aceptarse como “medios de cambio” parece apuntar hacia *tokens* fungibles, sin incluir los no fungibles. Además, los proveedores de servicios cripto incluidos en los artículos 2.1 g) y h) se limitan a los *exchange* de cambios de monedas virtuales por fiduciarias y los proveedores de servicios de custodia de monederos electrónicos. Por tanto, las

plataformas podrían no estar incluidas si se tiene en cuenta que se opera con *tokens* no fungibles y que no hacen intercambios de *tokens* por dinero de curso legal (por ejemplo, casos de pago en criptoactivos). Incluso, se podría discutir que las billeteras estarían obligadas a controlar los criptoactivos en custodia, pero no los NFT.

También cabría plantearse si los NFT, en caso de emplearse como obras de arte y venderse y comprarse en las plataformas de NFT, podrían estar sujetos a los requerimientos de blanqueo de capitales a través de los artículos 2.3) i) y j). Todo ello, en los siguientes casos:

*i) las personas que comercien con obras de arte o actúen como intermediarios en el comercio de obras de arte, también cuando lo lleven a cabo galerías de arte y casas de subastas, cuando el importe de la transacción o de una serie de transacciones relacionadas sea igual o superior a 10 000 EUR;*

*j) las personas que almacenen obras de arte, comercien con obras de arte o actúen como intermediarios en el comercio de obras de arte cuando lo lleven a cabo puertos francos, cuando el importe de la transacción o de una serie de transacciones sea igual o superior a 10 000 EUR.*

La posición defendida en este trabajo es que los NFT (como obras de arte) deben estar sujetos a la regulación europea de blanqueo de capitales vía aplicación por analogía de la regulación existente en materia de crimen financiero. Sin embargo, hay que recordar que los NFT como obras de arte son solo uno de los tantos usos que pueden tener. Además, su valoración bajo el concepto de arte hace que las plataformas sean sujetos obligados por el régimen simplificado, requiriendo menos exigencias en comparación con aquellos casos de dinero electrónico e instrumentos financieros. Por tanto, las plataformas de compraventa de NFT en principio estarían sujetas al régimen simplificado y no al financiero.

No obstante, atendiendo a la sustancia o utilidad que se le den a los NFT, e incluso atendiendo a la promoción que se haga de ellos, podría valorarse que estos puedan estar sujetos al régimen del MiCA. Es más, podría haber coyunturas en las que los NFT se verían incluso como similares a instrumentos financieros. En cualquiera de los dos casos, las plataformas de compraventa de NFT podrían estar sujetas a los requisitos establecidos para los proveedores de servicios de criptoactivos o incluso para entidades de servicios de inversión.

La cuestión aquí es qué circunstancias se han de dar y a partir de cuándo un NFT no regulado puede pasar a estar regulado. El considerando 11 de MiCA, parece indicar el criterio al establecer

*Las partes fraccionarias de un criptoactivo único y no fungible no deben considerarse únicas y no fungibles. La emisión de criptoactivos como fichas no fungibles en una amplia serie o colección debe considerarse un indicador de su fungibilidad. La mera atribución de un identificador único a un criptoactivo no es suficiente, en sí o por sí misma, para clasificarlo como único y no fungible. Para que un criptoactivo se considere único y no fungible, también los activos o derechos representados han de ser únicos y no fungibles. La exclusión de los criptoactivos únicos y no fungibles del ámbito de aplicación del presente Reglamento se entiende sin perjuicio de la consideración de dichos criptoactivos como instrumentos financieros. El presente Reglamento debe aplicarse también a los criptoactivos que parezcan únicos y no fungibles, pero cuyas características de facto cuyas características vinculadas a sus usos de facto los harían fungibles o no únicos. A este respecto, al evaluar y clasificar los criptoactivos, las autoridades competentes deben adoptar un enfoque en el que predomine el fondo sobre la forma, según el cual las características del criptoactivo en cuestión determinen la clasificación y no su designación por el emisor.*

Es decir, un NFT fraccional se considerará como fungible y, por tanto, estará sujeto al MiCA. Aquellas fichas no fungibles y no fraccionables quedarían fuera del MiCA y estarían expuestos a una posible futura regulación específica a estos efectos. Respecto a su posible clasificación y, por ende, a sus requerimientos regulatorios de emisión y provisión de servicios, los NFT probablemente podrían considerarse como *utility tokens*, sujetos a los requerimientos más livianos. En ciertos casos, podrían incluso valorarse como *tokens* referidos a activos (*Asset Reference Tokens* o ART).

En efecto, en estos nuevos considerandos, el MiCA también advierte que ciertos NFT podrían llegar a catalogarse como un instrumento financiero, en cuyo caso, tanto la emisión de estos como los servicios ofertados por las plataformas estarían sujetos a una multitud de requerimientos regulatorios derivados de la Directiva 2014/65/EU (MiFID II), el Reglamento (EU) 600/2014 (MiFIR), el Reglamento (EU) 596/2014 (Market Abuse Regulation), la Directiva 2014/57/EU (Market Abuse Directive) y el Reglamento (EU) 2017/1129 (Prospectus).

De cualquier modo, los *tokens* fraccionables deberán ir acompañados, como mínimo, de un libro blanco si están sujetos al MiCA y de un prospecto si son instrumentos financieros. Un *token* que nazca como fraccionado no tendría duda, pero puede darse la situación de que inicialmente se trate de un *token* único y que un posterior dueño en la cadena de compraventas decida crear fracciones de este. En este caso, el detonante de pasar de no regulado a regulado no sería originado por la emisión inicial, sino en el momento de la decisión de fraccionamiento. Este fue precisamente el caso que se dio en agosto de 2022, cuando un NFT de Cryptopunk (arte) que se vendió por primera vez en 2018 se fraccionó y se vendió a más de 56 000 contrapartes (Jenkinson, 2022, pp. 1-2).

Un efecto similar al de los NFT fraccionados puede darse en situaciones en las que un mismo emisor crea una colección de NFT similares y en gran volumen (hay que indicar que no existen limitaciones respecto al número de NFT de la misma colección que pueden emitirse y ponerse a la venta). Estos ejemplos se han identificado como creaciones en lote y pueden emplearse de formas similares a las de las ofertas iniciales de fichas o *Initial Coin Offerings* (ICO). Otro escenario de resultados similares a los de una ficha fungible o un instrumento financiero podría llegar a darse si se emitieran NFT que apuntaran o referenciaran a productos financieros, como acciones, bonos, seguros, créditos o incluso metales preciosos, puesto que, en estos casos, se estaría hablando de que las plataformas de NFT estarían negociando sobre productos financieros en su sustancia real.

En conclusión, los NFT no deben evaluarse únicamente con base en su clasificación como *tokens* no fungibles (ERC), sino que deben tratarse en función de cómo operan y la utilidad que se les da en la realidad. Esta utilidad no es estática, sino que fluctúa con el tiempo. Por tal razón, los emisores, los compradores, las plataformas de negociación de NFT y los proveedores de servicios auxiliares (por ejemplo, custodia de NFT) deben realizar evaluaciones sobre la naturaleza del NFT en el momento de su adquisición y en cada una de sus transacciones.

#### **4. Análisis crítico de los elementos de riesgo**

Una vez revisados y analizados los principales tipos de criptoactivos, es importante resaltar los principales elementos de riesgos asociados a ellos, identificando las categorías de gobernanza, los conflictos de interés, el crimen financiero, las protección de datos, la transparencia y la protección al consumidor, así como los riesgos operacionales y de ciberseguridad.



## 4.1 Gobernanza

La gobernanza o estructura de toma de decisiones respecto a los criptoactivos puede ser centralizada (una entidad puede identificarse como responsable de la toma de principales decisiones) o descentralizada, en cuyo caso no es posible identificar una entidad o un órgano decisor. Actualmente, estos segundos casos parecen estar fuera del ámbito del Reglamento MiCA y, por lo tanto, podría estar limitándose la oferta de estos servicios dentro de la zona euro, salvo que se interprete que estos casos entran en la definición general del artículo 3, pero su emisión no está regulada (tan solo su operativa a través de proveedores de servicios de criptoactivos).

Sin embargo, esta interpretación respecto a los criptoactivos de emisión descentralizada o no identificada abriría la discusión sobre si potencialmente los NFT entrarían dentro del ámbito del MiCA. Esto se debe a que la definición de criptoactivos contenida en el artículo 3.1 (5) del MiCA es tan amplio<sup>102</sup> que podría abarcar los NFT y, por tanto, la misma interpretación dada a las criptomonedas no emitidas por una persona identificable (*bitcoin*) podría extenderse a los NFT.

De ser así, podría argumentarse que las plataformas de oferta de NFT podrían catalogarse como proveedores de servicios de criptoactivos. Este punto debe discutirse, puesto que la posición de esta autora es que dichas plataformas solo se considerarían sujetos a la normativa del MiCA si ofertasen dentro de sus plataformas NFT con características financieras o que se estuvieran empleando como activos sujetos al MiCA o cualquier otra regulación financiera como pueda ser MiFID II. Una interpretación extensa podría llevar a que un supervisor financiero amplíe su mandato a aspectos que no son estrictamente financieros.

Con respecto a los modelos centralizados, se debe llevar a cabo un filtrado adecuado tanto de los fundadores o socios de la entidad cabecera como de los miembros de la alta dirección y los gestores de riesgos o *gatekeepers*. Pese a que MiCA European Commission, 2020 ya contempla este tipo de medidas, cabe plantearse cómo operarán en la práctica (Digital Asset Association Austria, 2021, p.1), dado que los filtrados de prensa negativa podrían excluir al propio Facebook (actualmente Meta) debido a las numerosas sanciones impuestas por asuntos relacionados con la protección de datos y el abuso de

---

<sup>102</sup> “criptoactivo: una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar” (art. 3.1 (5) MiCA).

posición dominante (Stauber, 2019, pp. 2-9). Asimismo, surgen cuestiones sobre qué sucedería si los miembros aprobados inicialmente emiten un criptoactivo que posteriormente se considera inválido, lo cual afectaría a la reputación del criptoactivo en sí mismo.

Del mismo modo, los requerimientos de conocimiento y experiencia de altos cargos y posiciones clave puede resultar complicado debido a la novedad de este tipo de modelos de negocio, que hasta ahora carecían de funciones de control como, por ejemplo, auditoría, riesgos o cumplimiento, por lo que podría darse escasez de profesionales adecuados para este tipo de posiciones. En consecuencia, sería conveniente homogeneizar criterios de adecuación y no restringir la necesidad de presencia física en la jurisdicción relevante, siempre que la persona se encuentre en la UE (Comisión Europea, 2020c, p.1). De lo contrario, algunos países tendrían problemas con la identificación de profesionales con las cualificaciones requeridas. Además, este tipo de negocios tiende a operar de forma remota con equipos deslocalizados.

La adecuada gobernanza en la toma de decisiones y su evaluación es otro de los elementos que deberá desarrollarse en detalle a través de los estándares técnicos de segundo o tercer nivel. En el caso de las criptomonedas estables referenciadas a cestas de divisas, los órganos decisores del emisor deberán establecer las proporciones, el tipo de activos que servirán como colaterales, así como las posibles sustituciones de estos en casos de falta de liquidez o cambios en las proporciones (art. 36 del MiCA). El propio mercado de las *stablecoins* ya ha sufrido casos de prensa negativa sobre este asunto, como el de Tether (CBINSIGHTS, 2021, pp. 1-19).

A este respecto, en lo que a *stablecoins* se refiere, en la actualidad se consideran como respaldo adecuado valores como depósitos en efectivo en bancos, custodios de criptoactivos o activos de alta calidad y liquidez (*High Quality Liquidity Assets* o HQLA) (Bank of International Settlements [BIS], 2020b, pp. 2-22). Estas opciones requieren que las instituciones donde se depositen los fondos no tengan una exposición alta a préstamos hipotecarios, con el fin de responder a los requerimientos de liquidez inmediatos (Gensler, 2019, pp. 1-32). Del mismo modo, los activos de bajo riesgo y alta calidad pueden tardar en deshacer posiciones, por lo que en un caso de ventas masivas urgentes o *fire sales* (Financial Stability Board [FSB], 2020e, p. 12), podrían no responder a la velocidad a la que se mueve el mundo cripto, necesitando, por lo tanto, medidas que funcionen como ralentizadores o cortafuegos (por ejemplo, desincentivar la conversión mediante

devoluciones con un porcentaje menor al ratio 1:1 entre la criptomoneda estable y la moneda de curso legal).

Otras opciones que no se contemplan en MiCA podrían incluir que las reservas de los emisores de criptomonedas estables se mantengan directamente en cuentas de bancos centrales (Panetta, 2020, pp. 1-5) o, incluso, en el futuro, respaldarse con monedas digitales de bancos centrales (CBDC) (Adrian et al., 2021, pp. 1-3). Este tipo de ideas ya se han implementado en casos como Alipay y WeChat en China. En ambos casos, los balances correspondientes a los fondos de los clientes se encuentran depositados en una cuenta del banco central del país. Como puede verse, a diferencia de Europa o Estados Unidos, las *FinTech* en China se conciben como miembros directos del sistema de pagos, compensación y liquidación, por lo que cuenta con la capacidad de operar directamente con el banco central (Adrian et al., 2021, pp. 1-3). Estas alternativas podrían dar mayor seguridad al público en general y, por tanto, apoyarían una mayor adopción de este tipo de criptoactivos, evitando las barreras a las que hasta ahora se ha enfrentado, como el *de-risking*<sup>103</sup> de los bancos e instituciones financieras.

Por otro lado, la posibilidad de que las grandes tecnológicas accedan a estos servicios se traduce en riesgos de conflictos de interés, protección a consumidores y protección de datos ya identificados y subrayados en capítulos anteriores<sup>104</sup>. En suma, tanto las estructuras accionariales como las organizaciones internas de los participantes principales deberán adoptar esquemas de filtrado de contrapartes con las que realicen negocios (diligencias debidas), deberán contar con un modelo de tres líneas de defensa (auditoría, cumplimiento y riesgos, negocio) y, a partir de ciertos volúmenes u operaciones, se hará necesaria la evaluación por auditores externos en distintas materias (principalmente asuntos financieros, de certificación de activos que operan como colateral, crimen financiero y ciberseguridad).

## ***4.2 Conflictos de interés***

La adecuada gestión de conflictos de interés en el ecosistema del criptoactivo y dentro de sus principales participantes es otro elemento que, hasta ahora, no ha gozado de la suficiente atención y que requerirá de un adecuado enfoque basado en riesgos. Estos

---

<sup>103</sup> *De-risking* financiero se define como “el fenómeno por el que instituciones financieras terminan o restringen las relaciones comerciales con clientes o categorías de clientes para evitar, en lugar de administrar el riesgo” (U.S. Department of State, 2021, p. 1).

<sup>104</sup> Ver el apartado “2. Los sujetos. *Las BigTech*”.

nuevos modelos pueden asociarse a problemáticas de conflictos de interés relacionados con estructuras internas y organizacionales no adecuadas, las cuales deben remediarse o mitigarse (OICV-IOSCO, 2020, pp. 1-31).

En efecto, las entidades deberán establecer una adecuada política de gestión de conflictos materiales, control de información privilegiada y prevención de abuso de mercado (Título VI de MiCA). Las casuísticas variarán en función del tipo de entidad de la que se hable. A modo de ejemplo, en los casos de los emisores de *stablecoins* basadas en cestas de activos, se deberán establecer controles en tomas de decisiones de cambios en las estrategias respecto a su composición, peso o mecanismos de estabilidad para evitar casos de inversiones ventajistas (*front-running*) (G7 Working Group on Stablecoins, 2019, pp. 7-27).

En la industria existen antecedentes relacionados con los conflictos de interés y los emisores de criptomonedas estables que compartían equipos gerenciales con *cripto exchanges* (casas de cambio cripto), levantando sospechas de manipulación del mercado en Estados Unidos (Casos Tether-Bitfinex) (CBINSIGHTS, 2021, pp. 1-19). Estos casos podrán evitarse con adecuadas guías de prevención y gestión de conflictos de interés.

La desastrosa combinación de conflictos de interés y falta de regulación se hizo patente en 2022 con el estallido del escándalo de la plataforma de negociación de criptoactivos FTX y su declaración de bancarrota. FTX emitió sus propias fichas, alterando artificialmente su precio y empleándolos como colateral para la obtención de financiación. Además, la plataforma no llevó a cabo una adecuada segregación de activos de clientes frente a recursos propios y, por tanto, operó con los activos de clientes sin su consentimiento (KPMG, 2022, pp. 4-5).

### ***4.3 Crimen financiero***

La esfera de crimen financiero es uno de los principales focos de preocupación en relación con la actividad de criptoactivos en general. En estos casos, se debe aplicar un enfoque basado en riesgos respecto a la identificación y monitorización de las

operaciones. En la zona europea, tanto la Quinta Directiva<sup>105</sup> como la Sexta Directiva<sup>106</sup> de prevención de blanqueo hacen referencia a activos virtuales; sin embargo, cabe señalar que el listado enumerado en el artículo 3.1 (16) de MiCA es más amplio que los contenidos en ambas directivas, por lo que no todas las actividades contenidas en el MiCA se encuentran recogidas en la actualidad bajo las obligaciones de prevención de blanqueo de capitales. Ello se hace aún más complicado teniendo en cuenta que el nuevo “*travel rule*”<sup>107</sup> somete a la práctica totalidad de las actividades contempladas en el artículo 3.1 (16) de MiCA a obligaciones relacionadas con la información que debe incluirse en las transferencias de criptoactivos, incluso cuando algunos de estos actores no están sujetos a registro.

Las discrepancias en la aplicación de medidas de crimen financiero ya existen en la actualidad. Un ejemplo de ello es la interpretación de los Estados Miembros a lo que se consideran operaciones ocasionales o de bajo valor. Debido a la falta de estandarización, se aplican requerimientos distintos, como la no identificación, la firma de un documento declarativo o incluso la realización de una diligencia debida completa, independientemente de si se trata de una operación ocasional de bajo valor (Comisión Europea, 2020c, p.1). Estos desequilibrios de niveles de control en la zona euro provocan casos de arbitraje entre jurisdicciones de la región, por lo que es necesaria la estandarización de medidas.

Algo similar sucede con las pruebas de vida en casos de identificación, verificación y demostración de vida por vía remota, donde en ciertos países el proceso puede ser totalmente automático y en otros se exige intervención humana, aumentando los costos operativos en esas jurisdicciones (Comisión Europea, 2020c, p.1).

Los diseños de sistemas de monitorización de este tipo de negocio dependerán de la actividad que realice el proveedor de servicios, el tipo de moneda gestionada (mayorista o minorista), la extensión, la frecuencia y los volúmenes de sus operaciones, así como las

---

<sup>105</sup> Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (Texto pertinente a efectos del EEE).

<sup>106</sup> Considerando sexto: “El uso de monedas virtuales presenta nuevos riesgos y desafíos desde la perspectiva de la lucha contra el lavado de dinero. Los Estados Miembros deben velar por que dichos riesgos se aborden adecuadamente”. (Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal)

<sup>107</sup> Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

jurisdicciones con las que se interactúe. Asimismo, los sistemas deberán desarrollar indicadores de nuevas realidades propias del mundo cripto como, por ejemplo, uso de mecanismos de anonimato como *tumblers* o *mixers*<sup>108</sup> (Financial Action Task Force [FATF], 2020b, pp. 1-32), o el empleo de prácticas de *crypto wash trading*<sup>109</sup> por parte de casas de cambio (Cong et al., 2020, pp. 1-50).

La prevención de fraudes será otro de los aspectos a monitorizar, con el fin de evitar casos de preventas de fichas, publicidad falsa o engañosa (OICV-IOSCO, 2020, pp. 1-31) u ofertas realizadas por entidades no autorizadas o incluidas en listas de fraude. La cuestión que se plantea en estos casos es cómo realizar filtrados transaccionales contra listas relacionadas con el blanqueo, el terrorismo o las sanciones financieras internacionales, debido a que la información compartida es relativa a claves y cantidades, pero no es posible identificar contrapartes. En concreto, las sanciones financieras internacionales exigen el bloqueo inmediato de la operativa. Lo mismo ocurre en el caso de las transacciones con países que están sujetos a restricciones en la movilidad de capitales, las cuales deben ser seguidas por los participantes en la industria financiera. Tanto las herramientas de monitorización de operaciones (*a posteriori*) como las de filtrado contra partes sancionadas (en vivo) requieren de una serie de datos para su adecuado funcionamiento.

En la actualidad se están desarrollando soluciones que permiten la transferencia de estos datos entre los proveedores de servicios de pago involucrados de forma segura (ya sea mediante API o protocolos de identificación virtual), pero se añade la complejidad de tener que determinar si las contrapartes se rigen por los requerimientos de campos de la zona euro u otros<sup>110</sup>, pudiendo trasladar ineficiencias operativas ya existentes en las infraestructuras de pago actuales hacia las cripto. A este elemento, se añadirían ineficiencias ya conocidas como el uso de caracteres irregulares, la falta de estandarización o los posibles truncamientos.

---

<sup>108</sup> Se trata de servicios ofrecidos para aumentar la privacidad y perder el rastro de los criptoactivos mediante la mezcla de fondos de criptodivisas (con origen ilícito) con otros, con la intención de confundir el rastro con la fuente original de los fondos.

<sup>109</sup> *Crypto wash trading* es una práctica de alteración de precios, mediante la activación de volúmenes de compras y ventas entre direcciones cripto que pertenecen a empleados, personas relacionadas o el propio *exchange cripto*.

<sup>110</sup> Los requerimientos regulatorios respecto a campos que viajan en la transferencia se conocen como *travel rule* y, en la actualidad, están regulados por el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849 (Texto pertinente a efectos del EEE)

Estos aspectos se agravan en casos de uso de *software* de billetera digital no alojada<sup>111</sup> (*non-custodial* o *unhosted wallet*) por parte de particulares, sin la necesidad de intervención de ninguna entidad sujeta, pudiendo transferir valor en criptoactivos entre pares y evadiendo este tipo de controles (Financial Action Task Force [FATF], 2020b, p. 18). A este respecto, la fallida propuesta de Diem consistía en la implementación de controles como parte de su protocolo, incluyendo el control sobre direcciones *Blockchain* sancionadas, control sobre direcciones IP asociadas a jurisdicciones sancionadas y límites a las billeteras digitales no alojadas (*unhosted*), entre otras medidas (Libra Association, 2020, pp. 1-29).

El siguiente paso natural a las actividades de conocimiento de clientes y monitorizaciones es la dinámica de informes a los organismos supervisores, ya sean informes ordinarios o informes *ad hoc* relacionados con operativas sospechosas. En estos mecanismos, la canalización de la industria cripto hace que sea necesario un replanteamiento de los formatos y criterios de escalado de informes, especialmente los de operativas sospechosas, puesto que difieren de país a país, tal y como muestran los estudios estadísticos, siendo España uno de los países con menor número de informes de Europa (Lagerwaard, 2018, pp. 1-22). Un potencial uso de las criptomonedas estables significativas podría disparar los volúmenes de los informes, requiriendo de soluciones automatizadas y reduciendo la carga humana o manual que en la actualidad exigen estos informes en ciertas jurisdicciones.

Por consiguiente, cabe justificar que la posición de esta tesis se encuentre en conflicto con afirmaciones tales como las de Morales Barroso, quien apuntó lo siguiente:

*La tecnología Blockchain se adapta muy bien a los métodos contra el lavado de dinero, al reducirse los costes del proceso que llevan a cabo las instituciones financieras para cada nuevo cliente, pues una vez verificados los datos se almacenan criptográficamente en la cadena de bloques, y se podrían compartir con otras instituciones para su verificación. También sería posible aumentar la*

---

<sup>111</sup> Las billeteras son *softwares* de interface de usuarios empleados para gestionar los criptoactivos en una *Blockchain*. Existen dos tipos, dependiendo de quién tiene control de las claves privadas: si es la propia persona, se trata de *unhosted wallets* o *non-custodial wallets*; y si se gestionan por un proveedor de servicios, son *custodial* o *hosted wallets* (Wharton School, Digital Asset Project, World Economic Forum, 2020, pp. 1-20). A su vez, pueden existir dos formatos: *hot storage wallet* (billeteras que están *online*) y *cold storage wallet* (billeteras *offline*).

*efectividad de la monitorización y el análisis de datos de transacciones monetarias.* (Morales, 2018, p. 64)

En la práctica, la automatización, el empleo de tácticas de evasión, ya sean *tumblers* o *mixers*<sup>112</sup>, junto con el empleo de criptodivisas privadas que aseguran el anonimato, y el uso de puentes para fraccionar y mover los criptoactivos hacia *blockchains* y proveedores de servicios de criptoactivos con menores niveles de control y monitorización, generan nuevos desafíos que requieren inversiones en soluciones, herramientas y formación. Sin embargo, estas medidas no son infalibles ante los retos actuales. Por lo tanto, la afirmación previamente mencionada de Morales Barroso puede parecer excesivamente positiva sin tener en cuenta la complejidad real que representan actualmente las *Blockchains* y los criptoactivos.

#### **4.4 Protección de datos, transparencia y protección al consumidor**

##### 4.4.1 Protección de datos

La protección de datos es objeto de preocupación respecto a los criptoactivos y, más específicamente, en propuestas presentadas por grandes empresas tecnológicas o consorcios de estas. A diferencia de los bancos tradicionales, este tipo de entidades no solo operan considerando fuentes de ingresos económicas, sino también los datos como fuente de riqueza. Por consiguiente, existe el riesgo de usar los datos con fines comerciales sin autorización previa (Panetta, 2020, pp. 1-5). Puede existir la posibilidad de búsqueda de consentimiento expreso para compartir datos entre empresas del grupo (Libra Association, 2020, pp. 1-29), pero debe tenerse en cuenta que, debido a que las entidades tecnológicas (especialmente las dedicadas a redes sociales) tienen un efecto de red importante, el usuario podría verse obligado a aceptar para no quedar excluido del servicio. Estos casos podrían acentuarse en colectivos especialmente débiles que carecen de cuentas y se verían obligados a aceptar los términos y condiciones que se les impusieran, con el fin de acceder a un servicio de billetera o de procesamiento de órdenes de pagos.

Por ese motivo, es necesario establecer criterios normativos de separación de datos entre: (i) entidades del grupo no reguladas y entidades que ofrezcan servicios relacionados

---

<sup>112</sup> Se trata de servicios ofrecidos para aumentar la privacidad y perder el rastro de los criptoactivos mediante la mezcla de fondos de criptodivisas (con origen ilícito) con otros, con la intención de confundir el rastro con la fuente original de los fondos.



con el mundo cripto y, (ii) para los casos similares a los de asociaciones como Libra, implementar controles sobre el traspaso de datos entre el ecosistema Diem y los miembros de la asociación, puesto que incluyen entidades de pago, tecnología y economía de plataformas, telecomunicaciones, servicios *Blockchain*, capital riesgo y organizaciones no gubernamentales (Marcus, 2019, pp. 1-7).

En cuanto a los modelos operativos, los proveedores de servicios de pago de cripto deben cumplir con las normativas de protección de datos existentes. Es necesario encontrar un equilibrio entre cumplir con los requisitos de prevención del blanqueo de capitales y la financiación del terrorismo, al mismo tiempo que se preservan los requisitos de privacidad. En la actualidad, se están desarrollando soluciones de protocolos que permitirían que la información viaje de manera segura y encriptada. En conclusión, el modelo del ecosistema en torno a la emisión y gestión de los criptoactivos debería diseñarse con estándares de privacidad desde el inicio, lo cual permitiría ajustar las medidas de control de la información.

#### 4.4.2 Transparencia y protección al consumidor

Dado que el potencial de expansión de los criptoactivos (en especial las *stablecoins* globales) es incluso mayor al de los propios bancos, es importante establecer estructuras adecuadas de transparencia hacia el público en general. Máxime si se tiene en cuenta que en el caso de Facebook uno de los propósitos de Diem era servir a poblaciones no bancarizadas o subbancarizadas (Libra Association, 2020, pp. 1-29), y que su nivel de conocimiento del mundo financiero es muy bajo o nulo.

En el caso europeo, se han establecido requerimientos de comunicaciones publicitarias<sup>113</sup> (arts. 29 y 53 de MiCA), información precontractual y postcontractual, incluyendo los denominados libros blancos de criptoactivos (principalmente art. 6, 12, 15, 19 de MiCA), que mostrarán toda la información necesaria para que los consumidores puedan tomar decisiones con conocimiento de causa. Todas ellas deben publicarse en la página web; sin embargo, no parecen ser obligatorias en las aplicaciones, cuando la mayoría del público tiende a usar los teléfonos inteligentes.

Debido a que el sector no está familiarizado con este tipo de documentos y su nivel de detalle, es posible que en etapas iniciales estos no alcancen el nivel de expectativas

---

<sup>113</sup> En España se publicó el proyecto de circular de la CNMV sobre publicidad de criptoactivos.

supervisoras requeridas, puesto que es probable que las autoridades empleen documentación con la que ya están familiarizados, como los *prospectus*. Existen otras políticas relacionadas con la protección de los consumidores que también deberán ser establecidas, como los procedimientos de presentación de quejas y reclamaciones (artículo 31 de MiCA), los canales de denuncia<sup>114</sup> (art. 116 de MiCA), la segregación de activos (art. 37 de MiCA) y mejor ejecución de órdenes (art. 78 de MiCA).

#### ***4.5 Gestión de riesgos operacionales y ciberseguridad***

A los habituales riesgos propios de la industria financiera (emisores de dinero electrónico, casas de cambio, proveedores de servicios de pago o custodios) se suman nuevos riesgos de tipo operacional y de ciberseguridad que se deberán gestionar y que hasta ahora la industria no estaba formalizando conforme a las expectativas supervisoras. En principio, se pueden destacar cuatro aspectos clave: (i) fraccionamientos y deslocalizaciones de la cadena de valor, (ii) un adecuado enfoque de diligencia debida a proveedores y contrapartes, (iii) capacidad de la infraestructura tecnológica y (iv) contexto de ciberseguridad.

Desde el punto de vista macroprudencial, las entidades y tecnologías involucradas en la gobernanza del criptoactivo pueden estar deslocalizadas en distintos países con diferentes niveles de exigencia respecto a la ciberseguridad y los controles de infraestructuras tecnológicas. En caso de darse una rápida adopción de estos ecosistemas como forma de pago alternativa en la UE, podría generarse una dependencia de los pagos europeos de tecnologías estructuradas de acuerdo con los criterios de menor confianza (Panetta, 2020, pp. 1-5).

Respecto al segundo aspecto clave, el adecuado conocimiento y filtrado de las contrapartes ha de tener en cuenta el riesgo que suponen. Para ello, se pueden abordar mecanismos de estandarización de proveedores de servicios de criptoactivos, como modelos diseñados por asociaciones de este tipo de colectivos que se tomen como ejemplos de buenas prácticas para la industria<sup>115</sup>, añadiendo revisiones periódicas de su situación regulatoria, operativa y de seguridad (Financial Stability Board [FSB], 2020c,

---

<sup>114</sup> Este artículo requiere la modificación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión

<sup>115</sup> Este tipo de modelos de diligencia debida, diseñados por miembros de la industria y acogidos *de facto* como estándar global, se dio en el pasado con los cuestionarios Wolfsberg para la banca corresponsal (Wolfsberg Group, 2020, pp. 1-17).

pp. 1-73). Asimismo, es necesario evaluar los riesgos de exposición o concentración en entidades que puedan tener distintos papeles dentro de la gobernanza del criptoactivo o de la provisión del servicio. Por ejemplo, se pueden dar casos de instituciones financieras que funcionen como custodio de la reserva, proveedor de billetera y revendedor (Financial Stability Board [FSB], 2020e, p. 12).

En lo referente a las infraestructuras tecnológicas y su capacidad, surge la duda de si son lo suficientemente robustas para soportar grandes volúmenes operativos en sistemas financieros más amplios (Financial Stability Board [FSB], 2020e, p. 12). Por este motivo, la evaluación de las capacidades tecnológico-operativas y sus posibles limitaciones es un aspecto que se debe incluir en el día a día de estas actividades, junto con planes de continuidad de negocio y gestión de desastres (arts. 34. 7 a 34.9 de MiCA).

En relación con los riesgos tecnológicos y de ciberseguridad, es importante establecer mecanismos de control desde la fase de planificación de las entidades para detectar a tiempo los defectos de diseño que puedan comprometer la infraestructura, los fallos en los nodos de validación o las debilidades relacionadas con la ciberseguridad (Financial Stability Board [FSB], 2020e, pp. 1-67). Entre estos nuevos controles de ciberseguridad, es conveniente incluir los procedimientos de actualización de los contratos inteligentes (Bullman, Klemm, & Pinna, 2019, pp. 1-55) o los procedimientos de gestión de casos de *soft* o *hard forks*. Asimismo, las guías emitidas por la International Organization for Standardization (ISO), la International Electrotechnical Commission (IEC), el National Institute of Standards and Technology (NIST) o la International Organization of Securities Commissions (IOSCO) podrán servir como base para implementar mejores prácticas en la industria (G7 Working Group on Stablecoins, 2019, p. 8).

Finalmente, al igual que en el supuesto del crimen financiero, se debe rediseñar el entorno de escalado e informe de incidentes operativos y de ciberseguridad a autoridades, para poder incluir nuevos escenarios que se puedan dar, tales como el robo de claves privadas.

## **V. MODELOS FINANCIEROS DESCENTRALIZADOS**

De manera similar al caso de *FinTech* 3.5, a continuación, se identifica y delimita el universo de servicios *FinTech* 4.0 (servicios de DeFi basados en tecnología *Blockchain*). Esta sección se estructura dividiendo de nuevo entre actividades de pasivo, activo, servicios de inversión y otros servicios.

## 1. Productos de pasivo: las billeteras y los pagos descentralizados

Las billeteras digitales del mundo descentralizado prescinden de los requerimientos de apoyarse en una cuenta o tarjeta controlada por una entidad autorizada del sistema financiero. El hecho de descargar el *software* permite operar directamente, siempre y cuando la contraparte cuente con una dirección cripto para enviar las criptodivisas. Este tipo de billeteras se denominan no-custodiadas o privadas, dado que prescinden de la necesidad de un tercero que custodie los fondos.

Conviene abrir un pequeño inciso para comentar que las billeteras no-custodiadas contaron la única referencia explícita que podía encontrarse en la versión de marzo de 2022, de propuesta europea del Reglamento MiCA, que añadió el artículo 61.7 sobre requerimientos de cumplimiento normativo y crimen financiero por parte de los proveedores de servicios de criptoactivos. Esta sugerencia no fue contemplada en la versión final publicada, por lo que, en la actualidad, no se aborda abiertamente la casuística de billeteras privadas o no alojadas. No deja de sorprender que, pese a que las billeteras son un elemento básico de la operativa cripto, no cuentan con ningún artículo de dedicación específica a estas.

Volviendo al concepto de billeteras cripto, estas permiten mantener y operar con distintas criptodivisas de forma natural, sin que existan costos por apertura de cuentas multidivisa. Existen diversas opciones de billeteras, tales como billeteras web (no requieren descarga), de escritorio (*desktop*) (se descarga y ejecuta en el ordenador), móvil (similares a las anteriores, se descargan en el teléfono móvil), *hardware* (similar a un USB, por ejemplo) o incluso de papel. En cualquier caso, se emplean para guardar las claves privadas de los usuarios, y pueden conectar con una *Blockchain* o varias. Además, pueden guardar no solo criptoactivos fungibles, sino también no fungibles (o NFT), por lo que pasan a tener una utilidad mucho más amplia que la de sus equivalentes en el mundo tradicional.

La elección del formato depende de diversos criterios, como los tipos de criptoactivos en propiedad, sus balances y los volúmenes empleados junto con la frecuencia de las operaciones, el nivel de conocimientos (tanto tecnológicos como de criptoactivos), los dispositivos habitualmente empleados, los niveles de seguridad y la privacidad buscados (University of Nicosia, 2022, pp. 14-21).

Las billeteras digitales con base en plataformas centralizadas o semicentralizadas pueden contar con requerimientos previos de identificación y conocimiento de clientes en función de la jurisdicción en la que estén asentadas. Sin embargo, en los casos de billeteras descentralizadas, los requisitos de identificación pueden llegar a ser prácticamente nulos. Asimismo, pueden existir las denominadas “billeteras calientes” (disponibles en línea) o “billeteras frías” (*offline*), siendo las primeras más propensas a ciberataques. En cualquiera de los casos, la operativa de pagos se simplifica enormemente, eliminando intermediarios, costes asociados al uso de estos y tiempos de espera, como puede verse en el ejemplo propuesto en la Figura 34. En casos extremos de total automatización, se podría potencialmente prescindir de entidades bancarias y cámaras de compensación y liquidación. En ese sentido, el único costo asociado sería el propio de validación de la operación en la *Blockchain* correspondiente.

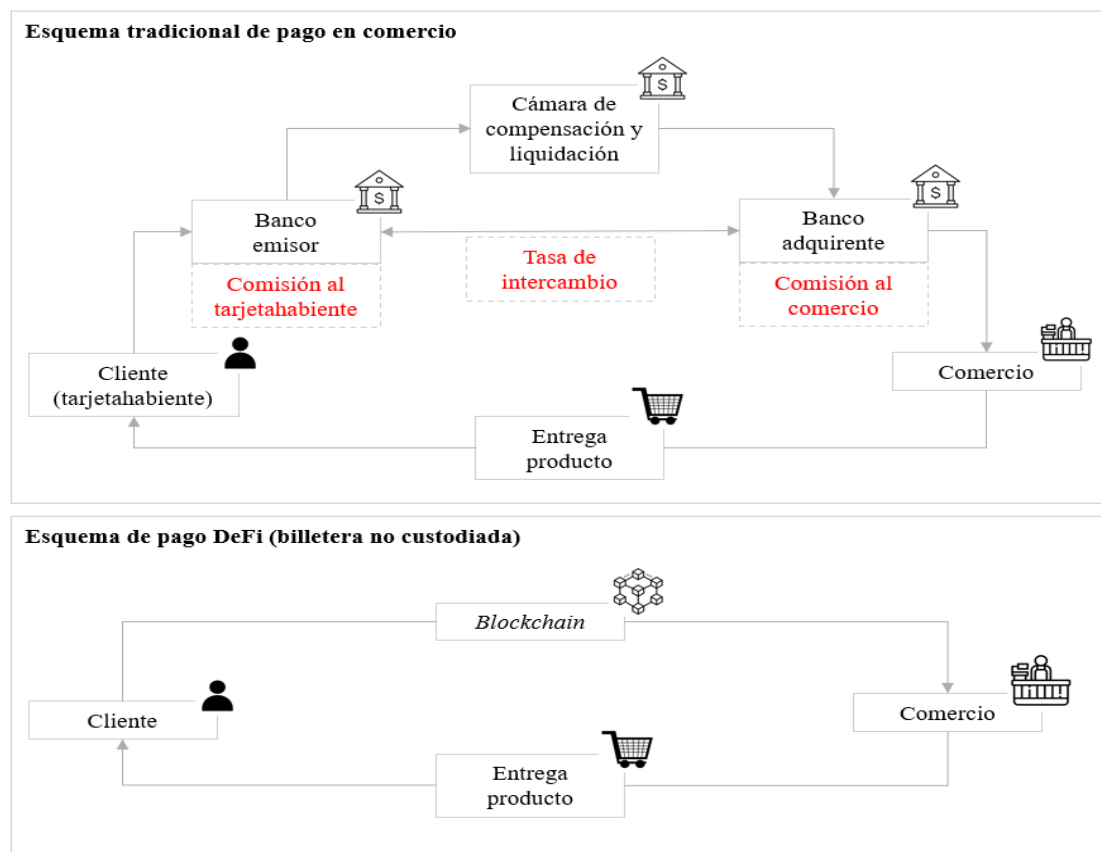


Figura 34. Comparativa de costos en los esquemas tradicionales de pago en comercio frente a hipotéticos esquemas de pago DeFi

Nota. Elaboración propia.

Actualmente, los servicios de pagos descentralizados cuentan con el potencial de ofrecer nuevas formas de pago, como puede ser el pago *streaming* ideado por el protocolo

Sablier (Sablier, 2021). Esta forma de operar se ideó principalmente para los trabajadores autónomos, quienes pueden realizar el pago alineado con el trabajo diario o en tiempo real, aunque también puede emplearse para cualquier tipo de transacción recurrente. De esta manera, no es necesario esperar al periodo habitual de pago (por ejemplo, mensual), sino que los reintegros se hacen por periodos definidos por las partes, llegando a diseñar liquidaciones por segundos.

Esta herramienta tiene un gran potencial en términos de inclusión financiera, puesto que ofrece una alternativa de obtención de fondos devengados por el trabajo sin necesidad de acudir a préstamos onerosos. Otro medio de operativa de fondos cripto son los cajeros automáticos cripto (o ATM cripto), siendo los más extendidos y conocidos los de *Bitcoin*. El crecimiento de los ATM experimentó un gran impulso desde 2020 aproximadamente. A modo de ejemplo, los ATM de *bitcoin*, el 1 de enero de 2020 eran 6352 y para el 19 de agosto de 2022 la cantidad se elevó a 38 663 (Coin ATM Radar, 2022).

Estos cajeros pueden ser unilaterales (solo se puede comprar *Bitcoin*) o bilaterales (se puede comprar y vender *Bitcoin*). Recientemente, aparecieron ATM que soportan varios tipos de criptoactivos. Aun así, estos ATM cobran comisiones que varían y, en la actualidad, no están sujetos a ningún tipo de requerimiento regulatorio. MiCA tampoco contiene ningún tipo de requisito para este tipo de operativas, pese a que, de extenderse el uso de criptoactivos en la UE, serían un canal más de interacción por parte del cliente.

## **2. Productos de activo: financiación descentralizada**

### **2.1 Crédito**

En el mundo DeFi, los créditos pueden catalogarse como colateralizados o no colateralizados. Los esquemas operativos descentralizados carecen de filtros de control, como puedan ser las comprobaciones relacionadas con el crimen financiero o con el riesgo de crédito que representa el solicitante. El detalle de dicha comparativa puede verse en la Figura 3535.

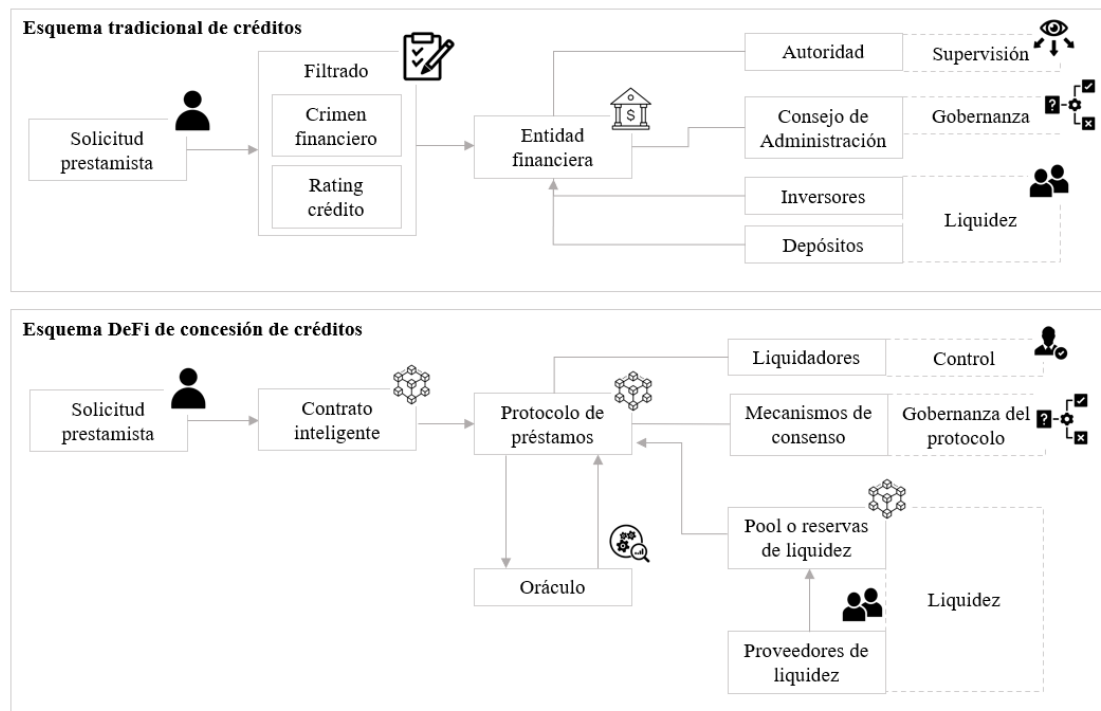


Figura 35. Comparativa de los esquemas tradicionales de crédito frente a esquemas DeFi

Nota. Elaboración propia.

Los créditos colateralizados son un instrumento habitual en las nuevas finanzas. En estos modelos, debido a la volatilidad de las monedas, se requiere un exceso de colateral de los criptoactivos que se bloquean en los contratos inteligentes con el fin de obtener la nueva criptodivisa (Aramonte et al., 2021, p. 27). De esta manera, los contratos inteligentes reemplazan al tercero de confianza. Debido al exceso de colateral que pone el solicitante, no se requiere realizar un análisis de crédito de este.

El solicitante tiene la opción de deshacer el crédito previo pago de una comisión, o el propio protocolo puede liquidar el préstamo cuando el valor del colateral caiga por debajo de los límites establecidos. En estos casos, el protocolo recupera el equivalente a la cantidad concedida más la comisión por liquidación. La cantidad restante se devuelve al prestatario. La propia lógica de la operación indica su uso residual con fines especulativos, puesto que el usuario solicita un préstamo, pero para ello aporta una cantidad (en otro criptoactivo) varias veces superior a la propia cuantía solicitada.

Recientemente, en noviembre de 2021, afloraron protocolos que sugieren soluciones de préstamos subcolateralizados en ratios de 1:3 mediante el juego de depósitos y préstamos a tipos fijos o a tipos variables. En concreto, la solución propuesta por el protocolo promotor Hashtack sugiere tres categorías de deudas, estableciendo sus

correspondientes rangos de liquidez. Cuando el ratio de liquidez se acerca a los niveles de liquidación, se realiza una llamada de liquidación que le brinda al deudor la oportunidad de aportar la cantidad necesaria para restablecer el ratio de liquidez entre el depósito y el préstamo. En caso de no hacerlo, el préstamo no se mantendría activo, sino que la cantidad depositada se liquidaría en un mercado automatizado o *Automated Money Market Maker* (AMM), cuyo rol se explica más adelante (Takahashi, 2021, pp. 2-15).

Estos productos descentralizados cuentan con las siguientes ventajas (McKinney, 2020, pp. 88-89): (i) el potencial de accesibilidad por parte de cualquier persona, independientemente de su localización; (ii) la eliminación de requerimientos de cambio de divisas con sus consiguientes costes; (iii) la automatización e inmediatez de la concesión de estos; (iv) el exceso de colateral requerido por el prestatario supone un colchón de seguridad para los prestamistas; y (v) la posibilidad de adaptar las condiciones a las necesidades de las partes. También cuenta con desventajas, dado que, por ejemplo, en casos de alta volatilidad de las criptomonedas, puede provocar su liquidación. Además, se añaden los riesgos propios del empleo de nuevas tecnologías, como la ciberseguridad de la propia plataforma respecto a posibles ataques a esta (McKinney, 2020, pp. 90-91).

Finalmente, los créditos no colateralizadas o *flash loans* consisten en la concesión del préstamo sin ningún requerimiento de identificación, análisis de crédito o colateral, siempre y cuando las cantidades se devuelvan dentro del mismo bloque de Ethereum (la operación se abre y cierra en una misma transacción) (Aave, 2022, p.1). En caso de no devolverse, la operación se revierte, como si nunca se hubiera prestado la cantidad. En Ethereum, se estaría hablando de unos 12 segundos de media entre la solicitud y la devolución del préstamo. Esto permite inferir que ninguna de estas opciones es factible para la compra de bienes o inmuebles, sino que se diseñaron con fines especulativos, específicamente para la búsqueda de beneficios derivados de arbitrajes en diferentes casas de cambio cripto.

Los *flash loans* también se han utilizado para realizar ataques a decisiones de gobierno de los protocolos y obtener beneficios económicos mediante la manipulación de los mercados, debido a que no existen limitaciones de cantidades a solicitar. Inicialmente, estos *flash loans* requerían conocimientos de programación (de hecho, se indicaban como una herramienta para desarrolladores); sin embargo, en la actualidad, existen herramientas para su uso por consumidores sin requerimiento de conocimiento de código (Aave, 2022, p.1).



En conclusión, el crédito en el ámbito de las DeFi es principalmente utilizado con fines especulativos y no satisface las necesidades de financiamiento de los ciudadanos comunes. Por lo tanto, no puede considerarse actualmente como un instrumento de inclusión financiera para poblaciones vulnerables. Es importante destacar que la regulación actual, como MiCA, no aborda específicamente la provisión de este tipo de servicios, ya sea por entidades descentralizadas o centralizadas.

## ***2.2 Initial Loan Procurements (ILP)***

Los *Initial Loan Procurements* (ILP) son una forma de financiación semejante al modelo de plataformas de financiación participativa en el mundo centralizado con monedas de curso oficial. Para los ILP, no hay inversores, sino prestamistas que no reciben fichas a cambio de su préstamo, sino intereses hasta la devolución de la cantidad prestada (Idaho Department of Finance, 2020, p.1). En estos casos, existe una combinación de firma digital de documentación legal (contrato de préstamo) junto con la versión del contrato inteligente en la *Blockchain*.

Por el lado de los promotores de los proyectos, su principal beneficio es que se prescinde de la emisión de una ficha requerida en los métodos de emisión cripto que se verán a continuación. Por el lado del prestamista, consiste en que, dependiendo del país, su tratamiento fiscal es más beneficioso que el de un instrumento de inversión y reciben intereses acordados por aportar sus criptoactivos (Fxempire, 2018, pp. 1-5). De modo similar al caso anterior, esta figura no se encuentra contemplada actualmente en el ámbito del MiCA.

## ***2.3 Crowdfunding descentralizado***

El *crowdfunding* descentralizado es la siguiente evolución al concepto *FinTech* de plataformas de financiación. Las plataformas de financiación analizadas en capítulos anteriores siguen basándose en el concepto de filtrado y centralización de operaciones. Como se pudo observar, estas plataformas realizan ciertas funciones como soporte de marketing, apoyo legal o coordinación de flujos, entre otros. A cambio, la plataforma se lleva comisiones en estos conceptos de gestión.

Además, en los modelos centralizados, las plataformas ponen en contacto a inversores o prestamistas cuyo perfil encaje con la solicitud de inversión, ya sea por la finalidad del

proyecto, el sector, las cantidades o los retornos. De esta forma, se limitan los inversores a los que los promotores acceden.

La propuesta de valor de la financiación participativa DeFi se basa en la descentralización, el acceso global (ausencia de filtros) y la total transparencia. Desde el punto de vista del promotor, esto se traduce en la reducción de tiempos en comparación con los filtros que ha de llevar a cabo una plataforma centralizada. Además, el contrato inteligente puede establecer el uso de los fondos, que deberá coincidir con lo que el promotor ha propuesto. Por este motivo, desde el punto de vista del inversor, resulta una solución atractiva debido a la transparencia en términos de uso de los fondos para el propósito que se ha prometido y con el desglose que se hubiera acordado entre las partes (Teslafan, 2021).

Como desventaja, se podría indicar que la financiación participativa descentralizada ofrece modelos de campañas y contratos, pero será labor del promotor el correcto diseño de la campaña de captación y documentación. Similar al caso del *crowdfunding* centralizado, existe un riesgo debido a la asimetría de la información respecto a la exposición al riesgo de crédito de los promotores, puesto que estos protocolos no acceden a la información de las deudas que el promotor pueda tener en el sistema financiero tradicional. Del mismo modo, el sistema financiero tradicional desconoce la exposición en el mundo cripto descentralizado. Como en los casos anteriores, esta figura no está regulada en el MiCA y la regulación actual de financiación participativa en EU no especifica casos de este tipo.

### **3. La transformación de los servicios de inversión**

#### ***3.1 Métodos de emisión cripto***

Las ofertas de fichas de valores negociables (*Security Token Offerings* o STO) pueden definirse como “una representación digital de un producto de inversión, registrado en un libro mayor distribuido, sujeto a la regulación del mercado de valores” (Lambert et al., 2020, p. 4). Por lo tanto, en este caso, las fichas se emiten otorgando derechos similares a los de los instrumentos financieros sujetos a la Directiva MiFID II y, en el caso español, a la Ley de Mercado de Valores, puesto que los inversores esperan una rentabilidad similar a las acciones, por ejemplo. En este contexto, la Ley del Mercado de Valores<sup>116</sup>

---

<sup>116</sup> Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión.

se modificó para poder incorporar el reconocimiento de valores registrados y operados sobre tecnología de registros distribuidos.

En caso de que la STO se oferte en el mercado europeo, quedará sujeta a ciertos requisitos equivalentes a las de los instrumentos de inversión, como la de la necesidad de intervención de un tercero autorizado para prestar servicios de inversión o la necesidad de emitir un folleto (*prospectus*) en caso de superar las condiciones establecidas en el artículo 35 de la Ley del Mercado de Valores, modificado por el artículo 6.5 de la Ley 5/2021 (Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores, 2015).

Pese a ello, hay un elemento de base que no parece encajar con el contexto de la MiFID II actual, esto es, el hecho de que las STO están basadas en DLT y carecen del requerimiento de la anotación en cuenta, ni operan por los circuitos tradicionales de compensación y liquidación. El Reglamento del régimen piloto DLT, que se aborda más adelante<sup>117</sup>, trata de solventar temporalmente estos choques o incoherencias regulatorias.

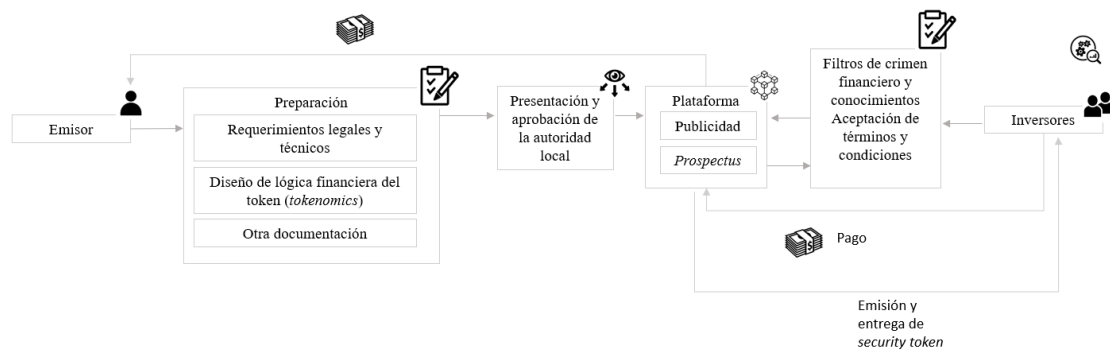


Figura 36. Esquema de operativa en Security Token Offering (STO)

Nota. Elaboración propia.

Las ICO son nuevas formas de financiación de compañías en estado incipiente, mediante la emisión de fichas a cambio de fondos, ya sea en divisas de curso legal o criptomonedas (European Securities and Markets Authority [ESMA], 2019, p. 11). En este caso, pese a que se otorgan beneficios, no existen expectativas de revalorización o evolución debido al proyecto que se financia, por lo que no hace parte del ámbito de aplicación de MiFID II (no se considera una ficha representativa de un instrumento

<sup>117</sup> Ver: AD-HOC MODEL OF DLT PILOT REGIME.

financiero, sino una ficha de consumo<sup>118</sup> o una ficha de pago<sup>119</sup>). Además, en los casos de las ICO, se espera que los receptores de las fichas operen con ellas, ya sea mediante el ejercicio de toma de decisiones o su consumo dentro del proyecto (Lambert et al., 2020, p. 6). Se puede ofrecer de diversas formas y a través de variados canales con un potencial de captación de fondos de cualquier país del mundo. Por este motivo, supone una fuente de preocupación desde el punto de vista supervisor y de protección a los consumidores (Su, 2020, pp. 2-24).

A diferencia de los modelos de financiación participativa, en las ICO no se requiere la intervención de una plataforma como parte imparcial entre el promotor o titular y el inversor, reduciendo los costos de este tipo de modelos de levantamiento de capital. Por su parte, los inversores ICO recibirán fichas representativas de capital, gobernanza, productos y servicios, o combinaciones de estos, según lo que se haya establecido entre las partes (ver ejemplo concreto de STO en la Figura 36).

Los términos de la emisión suelen estar descritos a través de documentos denominados *white papers* o libros blancos, que por lo general se publican en la web de la entidad. Su uso ha aumentado en los últimos años, puesto que representan una forma de reducción de costos, al prescindir de bancos y mercados de valores (European Parliament, 2021, pp. 1-9).

Las ICO se han regulado en la zona europea; a través del MiCA, con el fin de incluir premisas de protección a consumidores, transparencia y controles internos. Asimismo, se han emitido advertencias al público sobre los riesgos que presentan este tipo de actividades. En la UE, los promotores de los proyectos deberán someterse a registro ante la autoridad correspondiente.

Debido a que las ICO y las STO son zonas grises, a menudo incentivadas por el propio sector privado en su afán de evadir el caer en el ámbito de un instrumento de inversión y, por tanto, bajo regulación MiFID II, ha sido habitual que las partes interesadas esgriman que la emisión de sus *tokens* sea a través de ICO cuando en la práctica se trata de STO, o escalen sus dudas ante los supervisores. Así lo demostraron las estadísticas de consultas

---

<sup>118</sup> “ficha de consumo: un tipo de criptoactivo utilizado únicamente para dar acceso a un bien o un servicio prestado por su emisor” (art. 3.1.(9) de MiCA).

<sup>119</sup> Entendiendo que ficha de pago contiene tanto fichas de dinero electrónico como fichas referenciadas a activos en términos del Reglamento MiCA.

recibidas en el portal *FinTech* de la CNMV en 2020, con un total de 65 consultas acumuladas a diciembre de 2020, tal y como indicaba en su informe anual:

*En 2020 se ha producido un ligero aumento de las consultas recibidas en el portal, entre las que siguen destacando aquellas relacionadas con la tecnología Blockchain y, en especial, las que se refieren a proyectos basados en la emisión o negociación de criptoactivos. La falta de una regulación específica en materia de criptoactivos hace que existan dudas regulatorias en este tipo de proyectos. En concreto, en 2020 se recibieron 16 white papers de proyectos que solicitaban aclarar la naturaleza de los criptoactivos a emitir y, específicamente, si se trataba o no de valores negociables de acuerdo con los criterios de la CNMV. (Comisión Nacional del Mercado de Valores [CNMV], 2021, p. 326)*

El siguiente paso a las ICO son las *Initial Exchange Offering* (IEO), que consisten en la emisión de fichas a través de plataformas de intercambio de criptoactivos centralizados. De esta manera, los proyectos no solo obtienen financiación inmediata, sino que también la negociación de la ficha en la casa de cambio y, por tanto, la exposición a la circulación de la nueva ficha (Coinmarketcap, s.f., pp. 1-2).

Las *Initial Dex Offering* (IDO) son la progresión descentralizada de las ICO e IEO como forma de emisión de nuevas fichas. Actualmente, existen plataformas DeFi (casas de cambio descentralizadas o Dex) que permiten la emisión de IDO (por ejemplo, Uniswap o Binance). La figura a la que se podrían asimilar en el mundo centralizado podrían ser las plataformas de financiación participativa, prescindiendo de los controles propios de la plataforma y reemplazándolos por el criterio de supervisión de la comunidad.

Estos nuevos modelos ofrecen ciertos beneficios sobre las ICO e IEO, a saber: (i) los proyectos y *tokens* son evaluados por la comunidad, no por entidades, por lo que existe mayor posibilidad de financiación de pequeños proyectos; (ii) la estructura de las IDO facilita el acceso a liquidez, así como su uso mediante billeteras de la propia casa de cambio descentralizada, facilitando el flujo de las operaciones; (iii) la ausencia de necesidad de permisos; (iv) los inversores no tienen propiedad sobre el proyecto; (v) la carencia de comisiones por gestión de la emisión o requerimientos de obtención por parte de las fichas como comisión por la emisión; y (iv) la eliminación de limitaciones o requerimientos de exclusividad impuestos en los casos de las IEO. Sin embargo, debido

a la reducción de estas barreras, específicamente las de control, la posibilidad de riesgos de operativas fraudulentas aumenta en estos casos.

La posición de esta tesis es que las IDO no se encontrarían reguladas en el contexto del Reglamento MiCA, debido a que no hay una centralización ni del emisor ni de la plataforma, por lo que el futuro reglamento sufriría de este tipo de limitación en su publicación. Cabría plantearse si pudieran ser incluidas dentro del ámbito de aplicación de MiCA vía analogía, pero para ello deberían de desarrollarse indicios de cuándo una IDO se considera como suficientemente centralizada.

En general, los *Initial Token Offering* (ITO), ya sean centralizados o no, con propósito de ser un *token* de pago o una ficha equivalente a un instrumento de inversión, han sido objeto de críticas debido a ciertas malas prácticas. Estos escándalos se relacionan principalmente con fraudes en los que la emisión de las fichas era falsa, y los emisores vendían grandes cantidades en su posesión poco después del lanzamiento público, aprovechando los aumentos de precio y generando fuertes caídas para aquellos que no vendieron sus fichas a tiempo (generalmente el público que no estaba involucrado en el proyecto). Esta técnica se conoce como “*rug pull*”.

Estos incidentes también han sucedido en casos en los que las emisiones de los *tokens* eran legítimas, pero los miembros fundadores del proyecto vendían con fines especulativos (*pump and dump*) (Suárez, 2022, pp. 112-131). Estas casuísticas son similares a las que suceden en el mundo del capital riesgo tradicional. A este respecto, los supervisores más activos no han sido los europeos, sino los estadounidenses, quienes han criticado ampliamente la falta de responsabilidad por parte de los *crypto exchange* (tanto centralizados como descentralizados) en su rol de porteros o *gate keepers* a la hora de ofrecer la negociación de estas emisiones de fichas a través de sus plataformas (Nessa Risley vs Universal Navigation Inc. dba Uniswap Labs, 2022; SEC vs Poloniex, LLC, 2021).

Con el fin de mitigar estos riesgos, el propio mundo DeFi ha comenzado a experimentar con nuevas potenciales soluciones, como pueden ser las *Dynamic Coin Offerings* (DYCO). En el supuesto de la DYCO de MakerDAO, se fichas de consumo que estén respaldados (por ejemplo, por una criptomoneda estable o incluso por divisas de curso legal) durante un determinado periodo de vida útil del proyecto, permitiendo el reembolso de fichas de una forma segura (si el inversor no está de acuerdo con el rumbo que toma el proyecto, tiene la capacidad de devolver los *tokens* asignados, los cuales se

“quemar”, y recuperar el dinero invertido) (Coinmarketcap, 2022). Este respaldo en dinero de curso legal o *stablecoins* también permite una cobertura en evento de bajada del valor de los *tokens*, e incluso comienzan a aparecer variaciones que permiten extender esta seguridad en caso de transaccionar en mercados secundarios (Coinmarketcap, 2022, pp. 1-2).

Finalmente, las *Initial Farm Offerings* (IFO) son una nueva fuente de financiación, similar a las IDO, pero que buscan conseguir sinergias y optimización de beneficios entre los promotores del proyecto, la plataforma descentralizada y los inversores que ya tienen *tokens* propios de la plataforma descentralizada.

Bajo estos modelos, los inversores primero deben conocer la plataforma y comprar fichas de la plataforma o de la casa de cambio descentralizada (el caso más conocido es Pancake Swap y la ficha adquirida se llama Cake). Por otro lado, los promotores presentan sus proyectos, en los que indican cuánto van a necesitar y, dependiendo del modelo, indican en el propio contrato inteligente el valor o fondos que planean para el proyecto. Los dueños de fichas podrán aportar la cantidad en una piscina de liquidez y, una vez cerrada la ronda, se consumen las fichas aportadas a cambio de la emisión de *tokens* nuevos propios del proyecto.

De este modo, al quemar fichas de la plataforma, es decir, al consumirlos, se reduce la cantidad de *tokens* en circulación, provocando un efecto de subida del precio o valor de la ficha de la plataforma. Una vez más, la plataforma opera como un pseudobanco central gestionando la política monetaria de la plataforma, en estos casos denominada *tokenomics* (la lógica financiero-económica de las fichas de consumo que rigen en la plataforma) (Pancake Swap, 2022, pp. 1-2).

### **3.2 Exchanges descentralizados (casas de cambio) y Automated Money Market Makers (mercados de dinero automatizados)**

Al igual que en las casas de cambio centralizadas, en las casas de cambio descentralizadas los usuarios establecen órdenes de compra o venta a precios establecidos por ellos mismos o a precios de mercado. Sin embargo, en los *exchanges* descentralizados (Dex), los activos negociados no se encuentran en un tercero de confianza, sino que se encuentran en las billeteras de los propios usuarios, reduciendo los costos asociados a este tipo de operativas (Lau et al., 2020, pp. 75-76). En la Figura 37 se exponen las diferencias en flujos entre casas de cambio de divisas tradicionales y los Dex.

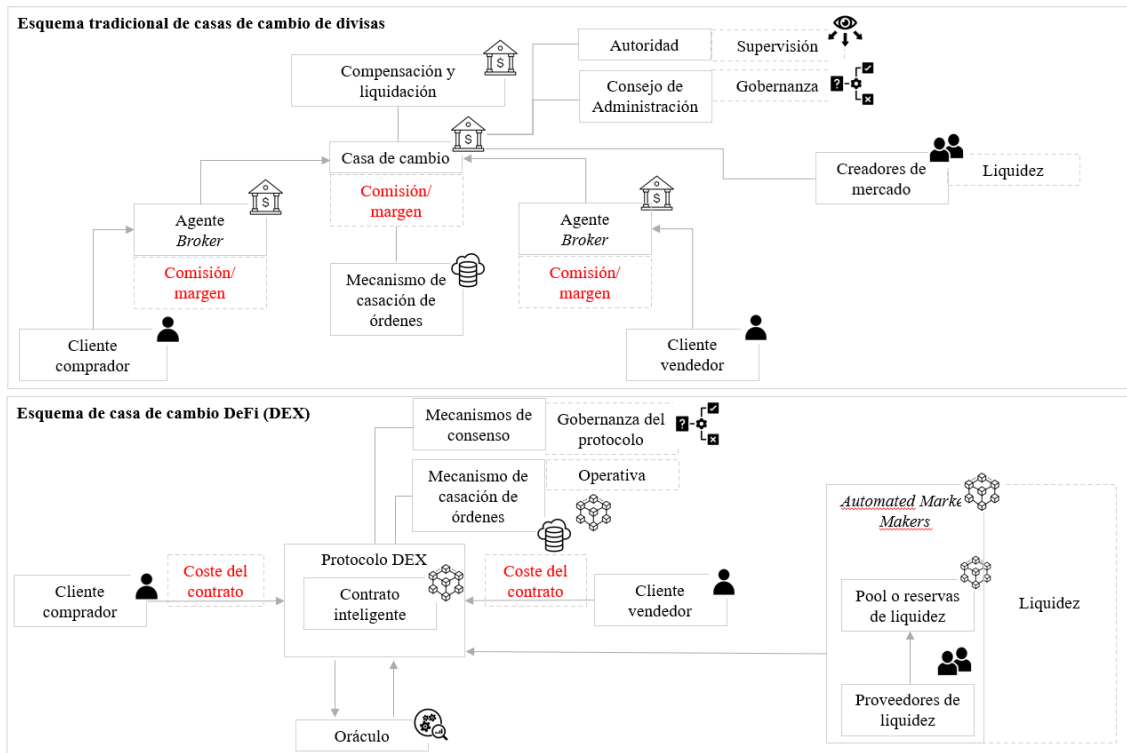


Figura 37. Comparativa de los esquemas tradicionales de cambio de divisas frente a esquemas DeFi

Nota. Elaboración propia.

Los *exchanges* siguen basándose en modelos de libros de órdenes, por lo que puede pasar tiempo hasta que las órdenes casen (Lau et al., 2020, pp. 75-76). La incertidumbre de la necesidad de espera o falta de liquidez de las casas de cambio es mitigada por los denominados AMM, mediante las figuras de las piscinas de liquidez o *liquidity pools*. Los AMM se definen como “conjuntos de activos con tipos de interés derivados algorítmicamente, basados en la oferta y la demanda del activo” (Compound, 2019, p. 1). Su esquema operativo de alto nivel se refleja en la Figura 38.



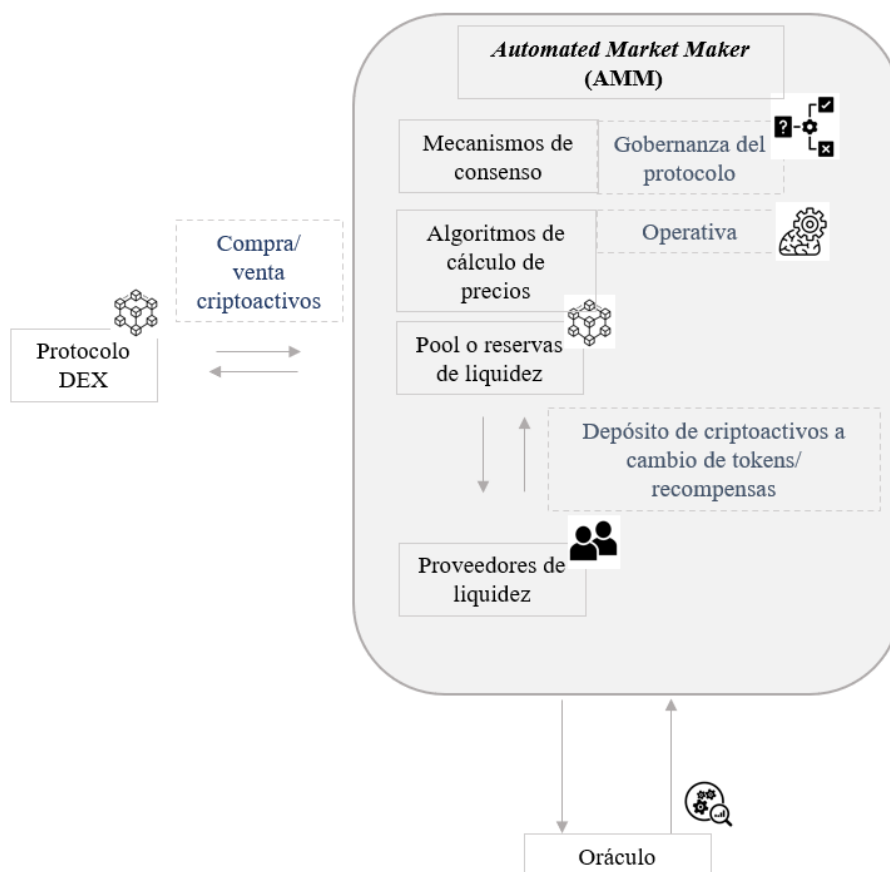


Figura 38. Esquema operativo de Automated Money Market Makers (AMM) en finanzas descentralizadas (alto nivel)

Nota. Elaboración propia.

En los modelos de AMM, los proveedores de liquidez depositan sus criptoactivos en las reservas de liquidez (piscinas de liquidez), recibiendo fichas propias de la plataforma como compensación (por ejemplo, en el supuesto de Compound, los prestamistas obtienen los denominados *cToken*) (Compound, 2019, pp. 1-8). Los prestamistas premiados en función de la cantidad y tiempo que los mantengan mediante intereses, pero en general podrán redimir sus fichas cuando ellos consideren. Esa liquidez es posteriormente usada para la concesión de préstamos por parte de la plataforma, previo depósito del colateral correspondiente por parte de los prestatarios. Ejemplos de AMM son los casos de Aave y Compound.

De esa manera, los AMM vienen a reemplazar la figura centralizada que representan los bancos tradicionales, al ser fuente de financiación y, a su vez, herramienta de depósito o inversión por parte de los proveedores de liquidez. Ambos modelos, Dex y AMM, pueden diseñarse de forma agnóstica a las distintas *Blockchain*. A este respecto, se realizó

un análisis de un total de 18 Dex y 8 AMM con un valor total bloqueado por encima de un billón de dólares a 24 de diciembre de 2021 con base en la información de Defilama.com (ver Tabla 11). Del total de la muestra de 26 casos, se identificó que existen más Dex con valores totales bloqueados cumpliendo el criterio en comparación con el número de AMM. Además, se identificó que un 30,77 % de la muestra opera en más de una cadena de bloques.

A su vez, se identificaron cadenas de bloques menores, con dependencia en un reducido número de Dex y AMM, que concentran los valores bloqueados, produciéndose, en estos casos, un riesgo de concentración en una reducida cantidad de participantes (por ejemplo, Terra). Esto provoca que, si estos protocolos sufren ataques o llevan a cabo malas prácticas como la manipulación de mercados, el riesgo de impacto en *Blockchain* más débiles sea mayor.

Motivos como este y el escándalo antes comentado de FTX han hecho que los reguladores a nivel mundial hayan puesto su foco normativo y de supervisión en este tipo de contrapartes. Si bien normativamente las acciones siguen centrándose en agentes proveyendo este servicio de forma centralizada, ciertos supervisores más activos, como el americano, han comenzado a expandir sus perímetros hacia Dex, como ha podido observarse en el caso de Uniswap, buscando nuevos indicios de centralización o toma de decisión para poder identificar a las contrapartes responsables del incumplimiento.

Tipo	Nombre	Valor total bloqueado a 24.12.2021 (billones de dólares)	Cadenas																				SUBTOTAL		
			Ethereum	Avalanche	Fantom	Arbitrium	Polygon	xDai	Harmony	Optimism	BSC	Moonriver	Celo	OKExChain	Palm	Heco	Terra	Tron	Solana	DeFiChain	Ronin	Cronos		Elrond	Binance
DEX	Curve (CRV)	\$22.68b	Si	Si	Si	Si	Si	Si	Si																7
DEX	Uniswap (UNI)	\$9.09b	Si			Si	Si			Si															4
DEX	PancakeSwap (CAKE)	\$5.67b									Si														1
DEX	SushiSwap (SUSHI)	\$5.45b	Si	Si		Si	Si	Si	Si		Si	Si	Si	Si	Si										12
DEX	Balancer (BAL)	\$3.21b	Si			Si	Si																		3
DEX	Trader Joe (JOE)	\$2.3b		Si																					1
DEX	Terraswap	\$2.13b														Si									1
DEX	SUNSwap (SUN)	\$1.68b															Si								1
DEX	Raydium (RAY)	\$1.67b																Si							1
DEX	DefiChain (DFI)	\$1.56b																	Si						1
DEX	Serum (SRM)	\$1.5b																Si							1
DEX	MDEX (MDX)	\$1.41b									Si					Si									2
DEX	Bancor (BNT)	\$1.38b	Si																						1
DEX	Katana	\$1.36b																				Si			1
DEX	VVS Finance (VVS)	\$1.33b																				Si			1
DEX	Astroport	\$1.29b														Si									1
DEX	Maia Exchange (MEX)	\$1.09b																					Si		1
DEX	BiSwap (BSW)	\$1b																					Si		1
AMM	AAVE (AAVE)	\$15.23b	Si	Si			Si																		3
AMM	Compound (COMP)	\$10.06b	Si																						1
AMM	Anchor (ANC)	\$9.01b														Si									1
AMM	Abracadabra (SPELL)	\$6.15b	Si	Si	Si	Si																			4
AMM	CREAM Finance (CREA)	\$2.13b	Si	Si	Si		Si				Si														5
AMM	Venus (XVS)	\$2.08b									Si														1
AMM	JustLend (JST)	\$1.79b															Si								1
AMM	Benqi (QI)	\$1.73b		Si																					1
	<b>SUBTOTAL</b>		9	7	3	5	6	2	2	1	5	1	1	1	1	2	3	2	2	1	1	1	1	1	

Tabla 11. Análisis de Dex y AMM y su operativa en distintas Blockchain a 24 de diciembre de 2021

Nota. Elaboración propia.

### 3.3 Gestión de carteras o gestión de activos

Los protocolos de gestión de carteras descentralizados surgieron principalmente como una herramienta de automatización de la gestión de las carteras de préstamos u otros activos y de las diferencias de tipos de cambios que ofrecen las casas de cambio descentralizadas. Su finalidad principal es la de una mejor gestión de la situación patrimonial de los usuarios, permitiéndoles general mejores retornos en sus inversiones.

Similar a los casos del mundo centralizado, la gestión de carteras del mundo descentralizado presenta soluciones de optimización de la cartera con base en las preferencias de los usuarios, teniendo en cuenta elementos como su apetito al riesgo, las previsiones de diversificación de la cartera y los horizontes temporales previstos (Wharton School, Digital Asset Project, World Economic Forum, 2020, pp.1-20). Como se observa en la Figura 39, a diferencia de las CeFi, la gestión de carteras o activos descentralizados prescinde de elementos de filtrado y no requiere de un vehículo de inversión específico o de interacción con *asset managers* o gestores de patrimonios.

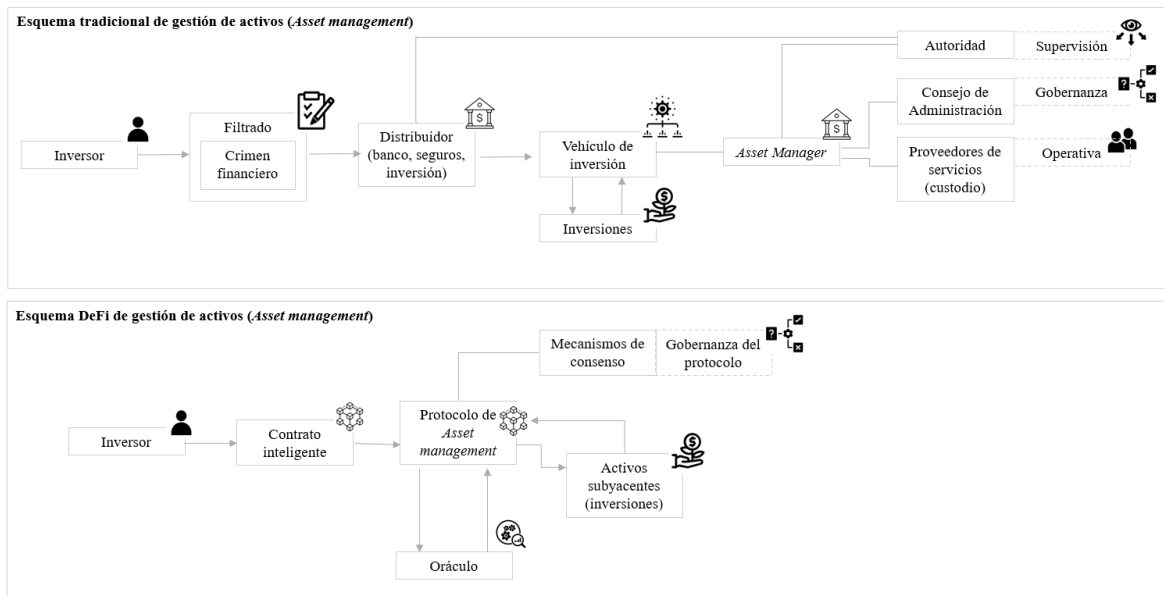


Figura 39. Comparativa de los esquemas tradicionales de gestión de activos frente a esquemas DeFi

Nota. Elaboración propia.

Los algoritmos de los protocolos realizan las negociaciones de forma automática sin requerir de intervención humana de forma intensiva (*robo sets*). En ciertas plataformas, como Tokensets, también existe la posibilidad de que los usuarios opten por seguir las

estrategias que hayan implementado los *top traders* de la plataforma, llevando, de esta forma, el conocido *social trading* al mundo DeFi (Lau et al., 2020, pp. 106-107).

En estos casos, los roles del mundo tradicional, como los gestores de carteras, asesores de inversiones, gestores de inversión e incluso más recientemente los *robo advisors* (asesores automatizados), se reemplazan por contratos inteligentes que automáticamente consultan oráculos de precios para decidir compras o ventas con el objetivo de optimizar la cartera del usuario de acuerdo con los parámetros previamente establecidos por este (ver Figura 39).

En este contexto, el riesgo principal es que los diseños de los algoritmos empleados no son auditados en los casos de protocolos descentralizados. Si bien se puede argumentar que la tecnología es transparente y sujeta a auditoría de la comunidad, los conocimientos tanto de programación como financieros requeridos para realizar estas tareas hacen altamente improbable que el ciudadano de a pie sea capaz de asesorar su adecuación previo al uso del protocolo. Además, el hecho de que la revisión del código esté abierta a la totalidad de la comunidad supone un riesgo en sí, puesto que está en manos de la persona que detecte vulnerabilidades el decidir si reportar con el fin de mejorar el código o si explotar la deficiencia en beneficio propio.

### **3.4 Agregadores de rendimiento**

Los agregadores de rendimiento se definen como “un conjunto de contratos inteligentes (llamado “protocolo”) que agrupa fondos de los inversores y los reinvierte en una variedad de productos que producen rendimiento o servicios mediante la interacción con sus respectivos protocolos” (Cousaert et al., 2021, pp. 1-14). Se trata de versiones evolucionadas de las gestoras de fondos.

Los agregadores DeFi son plataformas que se encuentran adaptadas a usuarios finales, de tal manera que agrupan diversas casas de cambio y proveedores de liquidez descentralizados. De esta forma, los usuarios pueden comparar y optimizar sus estrategias de inversión sin moverse de una misma plataforma, por lo que reducen costos y comisiones. Estas plataformas pueden ser agnósticas a la *Blockchain* en la que se opera y, por tanto, agrupar casas de cambio y AMM de distintas cadenas (Matcha, s.f.).

Los agregadores son empleados principalmente por aquellos usuarios que buscan obtener rendimientos de las diferencias de los precios ofertados en distintos *exchange* o

AMM sin necesidad de comparar manualmente. Ejemplos de agregadores DeFi son Zapper, Matcha, Idle Finance, Vesper o Yearn Vault.

Uno de los principales peligros del uso de estos agregadores es el hecho de que, de nuevo, se trata de un frontal con apariencia de unidad, pero que en realidad cuenta con numerosos elementos con su propia gobernanza y riesgos (cada una de las cadenas, cada uno de los *exchanges* y AMM con los que operan, los productos de estos, los oráculos que emplean para cada producto y los riesgos de una inadecuada programación de los contratos inteligentes). Estas contingencias son análogas a las que presentan en el mundo centralizado las *FinTech* que operan en modelos de BaaS o FaaS.

Esta vulnerabilidad es aún pequeña debido a los bajos volúmenes con los que se operan en comparación con los mercados financieros tradicionales. Sin embargo, en caso de usos masivos, aún no existen soluciones normativas regulando estos servicios DeFi, al menos en el espacio económico europeo.

### ***3.5 Derivados y predicción de eventos***

El mercado de derivados aumenta la diversidad de su oferta de servicios dentro de las DeFi al añadir a los ya existentes derivados de acciones, mercados, derivados, tipos de interés o activos elementos nuevos como los criptoactivos o predicciones de eventos.

Dentro de estos modelos se encuentran los casos de activos sintéticos (*synths*): activos o combinación de estos que equivalen a otros (activos del mundo *off chain*, como, por ejemplo, metales preciosos o del mundo cripto, como criptoactivos) en su valor en relación correlacional positiva (*normal synths*) o en relación correlacional negativa (*inverse synths*) (Lau et al., 2020, pp. 96-97). Este seguimiento se realiza a través de los denominados oráculos, los cuales se analizan más adelante. Los oráculos son terceros verificadores, ya sea mediante protocolos o a través de medios fuera de la cadena (automatizados o no). De esta manera, los usuarios manejan la exposición al precio del activo subyacente sin requerir de la tenencia de este en sí y pueden negociar su intercambio con una mayor eficiencia (Lau et al., 2020, p. 97).

Los protocolos de predicción de eventos o mercados predictivos son herramientas descentralizadas que permiten crear mercados sobre cuestiones futuras. Los participantes pueden invertir sobre el resultado que esperan que suceda en el escenario propuesto. Los

dueños de los *tokens* de gobernanza de los protocolos se encargan de validar el resultado final del evento a modo de ente descentralizado que verifica el resultado.

Si bien existe el riesgo de que los dueños de los fichas de gobernanza se pongan de acuerdo para dar un resultado diferente, este riesgo se mitiga mediante el reparto de fichas o comisiones por sus validaciones correctas o la retirada de los *tokens* que poseen en caso de detectar que han mentido. La misma propiedad de las fichas hace que los verificadores estén interesados en que estos suban de valor y esto se alcanza a través de validaciones correctas (Peterson et al., 2021, pp. 1-16).

## **4. Otros servicios**

### ***4.1 Servicios fundacionales: custodia de criptoactivos***

La custodia de criptoactivos es uno de los pilares fundamentales para la entrada de las instituciones y bancos tradicionales en el mundo cripto. En este encuadre, se considera que esta actividad se centra en la custodia de claves privadas en nombre de un tercero, dado que dicha clave representa la propiedad del criptoactivo y la posibilidad de gestión de este (por ejemplo, su transferencia). MiCA define este servicio en su artículo 3.1 (17) como “la guarda o el control, por cuenta de clientes, de criptoactivos o de los medios de acceso a esos criptoactivos, en su caso en forma de claves criptográficas privadas”. De hecho, la pérdida de la clave privada implica la pérdida del criptoactivo incluso por su legítimo propietario (Global Digital Finance, 2022, p. 2).

Los servicios tradicionalmente ofertados por los custodios<sup>120</sup> sufren simplificaciones en el mundo cripto (por ejemplo, reemplazo de actividades manuales que son automáticas a través de contratos inteligentes) y, en otros casos, se ven alterados. Asimismo, se conciben como servicios de seguimiento de cambios o riesgos propios de las fichas (mecanismos de consenso que impacten criterios de liquidación, *forks*, y criterios de minería) o incluso servicios de diligencia debida sobre los criptoactivos custodiados (detección de debilidades y técnicas que pongan el riesgo al cliente) (Global Digital Finance, 2022, p. 3).

---

<sup>120</sup> Esto es, a grandes rasgos, tenencia en custodia y salvaguarda de distintos tipos de activos, organización de liquidaciones y compensaciones, gestión de ingresos (por ejemplo, dividendos), administración de impuestos, provisión de información y servicios generales auxiliares.

Si bien cabe una absoluta descentralización de esta (el usuario custodia sus propios criptoactivos), existe también la posibilidad de delegación en un tercero de dichos activos, siendo estos los denominados “custodios de criptoactivos”. Su razón de ser subyace en la necesidad de diversos participantes de asegurarse unos adecuados niveles de salvaguarda de activos, así como una segregación de activos de los inversores a los que ofrecen sus servicios (por ejemplo, las casas de cambio, proveedores de liquidez y fondos de inversión deben segregar los activos de clientes) (Anchorage Digital, 2022, pp. 1-60).

En el escenario actual, existen, a grandes rasgos, dos posibilidades: el considerar que un banco custodio tradicional bajo la regulación existente tendría la capacidad de custodiar criptoactivos o el acudir a las nuevas *FinTech* que ofrecen dicho servicio pero que, a menudo, no se encuentran reguladas ni supervisadas o han optado por soluciones de licencias livianas o intermedias. Respecto a la primera opción, los bancos custodios regulados en la UE se han mostrado reacios a interpretar extensiones de los marcos normativos (principalmente MiFID II, AIFMD<sup>121</sup> y UCITS<sup>122</sup>) con el fin de ofrecer servicios cripto a sus clientes.

Por otro lado, los requerimientos de custodia cripto están limitados a aquellas fichas contempladas en MiCA, no quedando claro qué criterio aplica a la custodia de instrumentos financieros digitales o *tokenizados*, ya que están fuera del ámbito de aplicación del reglamento, pero la actividad y riesgos en custodia son equivalentes a los de MiCA, por lo que habría de interpretarse un solapamiento de requerimientos de custodia de instrumentos financieros tradicionales más aquellos nuevos contemplados en MiCA.

La reticencia se debe a que, pese a que los bancos custodios en la actualidad cuentan con medios para la custodia física y electrónica (especialmente tras la desmaterialización de instrumentos financieros como las acciones), la tecnología tras los servicios cripto es de tipo criptográfico, presentando problemáticas distintas a las vistas hasta ahora. Además, estos servicios de custodia se encontraban en un limbo regulatorio sin quedar claras las expectativas supervisoras. No solo esto, sino que también existen diferencias

---

<sup>121</sup> Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) N.º 1060/2009 y (UE) N.º 1095/2010. Texto pertinente a efectos del EEE.

<sup>122</sup> Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM).



operativas que deben valorarse, como, por ejemplo, el hecho de que no existe la necesidad de compensación de los criptoactivos, existiendo un registro descentralizado, por lo que ciertas figuras de los procesos operativos tradicionales devengarían innecesarias.

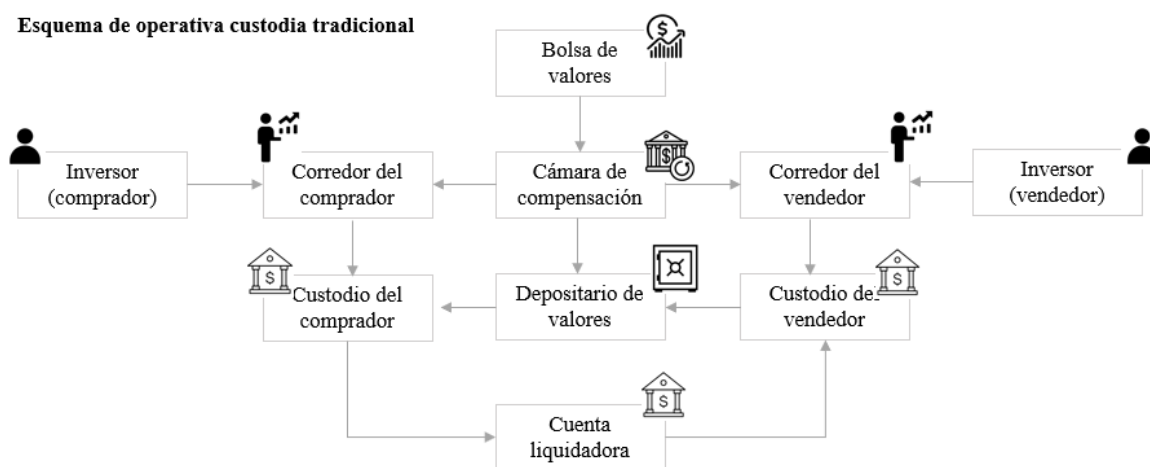


Figura 40. Esquema operativo de servicios de custodia tradicionales

Nota. Tomado de *A Market Overview of Custody for Digital Assets. Digital Custodian Whitepaper*, por Deloitte y Dubai Financial Services Authority, 2022, p. 5, Deloitte.

Además, en estos casos, el objeto de custodia son las claves privadas de los clientes, que, a su vez, son la evidencia de la propiedad del criptoactivo. Dichas claves criptográficas pueden mantenerse en distintos medios: papel, en línea o incluso *offline* (almacenamiento en frío). Dependiendo del medio en el que se custodien las claves y los controles implantados, será más difícil mostrar un control exhaustivo de estas (Anchorage Digital, 2022, pp. 1-60).

Por otro lado, han ido apareciendo *FinTech* cuya experiencia está centrada en la custodia de criptoactivos, pero, por lo general, no se encuentran regulados o supervisados, por lo que no es fácil evaluar la solidez de sus entornos de gobernanza y controles (especialmente la segregación de activos virtuales), transparencia o capacidad de respuesta ante incidentes. Cabe señalar que, dentro del mundo *FinTech*, la custodia de *tokens* puede darse como servicio único (custodia en sí) o combinado, como es el caso de la mayoría de las plataformas de negociación de criptoactivos, que a su vez custodian los fondos de sus usuarios (en su mayoría, a través de billeteras en línea en las que las plataformas mantienen en su poder las claves privadas y, por tanto, custodian el activo digital, cayendo en riesgos de concentración y conflictos de interés).

Las *FinTech* de custodia pueden ofrecer distintas soluciones, cada una con sus puntos fuertes y débiles. Por ejemplo, las soluciones de custodia en línea permiten una mayor accesibilidad, pero presentan un mayor riesgo de robo o mal uso. Para compensar, se pueden plantear soluciones de control, tales como el acceso y la operación a través de multifirma (varios usuarios deben firmar para que el acceso u operación se lleve a cabo) o agregando factores de autenticación reforzada similares a los implantados por la PSD II, siendo uno de ellos un componente biométrico.

Respecto a la custodia *offline*, se considera la más segura desde el punto de vista del custodio y la salvaguarda de criptoactivos; sin embargo, es la más complicada de reconciliar con aspectos como, por ejemplo, la necesidad de uso en caso de votaciones o uso con fines de *staking*<sup>123</sup>, obtención de *airdrops*<sup>124</sup> o incluso en casos de bifurcaciones (Anchorage Digital, 2022, pp. 1-60).

La razón de ser de este tipo de servicios en el mundo cripto es bastante similar al de sus análogos en el mundo tradicional: (i) reducir el riesgo y la complejidad del control de estos activos, (ii) el empleo de medidas de seguridad especializadas, (iii) la posibilidad de reclamo y recurso (en caso de custodios con licencia y asegurados), (iv) los servicios de custodia de criptoactivos en exclusividad ofrecen mayor seguridad que los de las plataformas de negociación, puesto que estos se exponen a mayores riesgos de *hacking* y, en muchas ocasiones, no aplican una segregación adecuada de activos de clientes, y (v) la mejor eficiencia operativa (Deloitte y Dubai Financial Services Authority, 2022, p. 8).

Uno de los principales puntos abiertos respecto a la custodia de criptoactivos es el hecho de que los protocolos y controles a aplicar dependerán de la categorización que se haga de estos (instrumento de pago, instrumento de inversión o arte digital) (Deloitte y Dubai Financial Services Authority, 2022, p. 10). Sin embargo, las fichas pueden servir varios propósitos al mismo tiempo o evolucionar de una categoría inicial (instrumento de pago) hacia otra (instrumento de inversión).

Esto se complica aún más si se tiene en cuenta que distintas jurisdicciones están aplicando criterios dispares (o no regulado), y si se añade el hecho de que muchos de los custodios de criptoactivos no están localizados en la zona europea, sino en países terceros

---

<sup>123</sup> El *staking* consiste en adquirir criptoactivos y bloquearlos (pignorarlos) con fin de recibir ganancias o recompensas (ya sea en dinero de curso legal o en criptoactivos) (Bit2me, 2022b, p.1).

<sup>124</sup> Los *airdrop* son repartos y asignaciones gratuitas de criptoactivos, por lo general con fines promocionales y de marketing para dar a conocer la ficha a la mayor cantidad de público posible y comenzar la circulación de este (Bit2me, 2022b, p.1).

como Estados Unidos, Reino Unido, Suiza o Singapur (Global Digital Finance, 2022, pp. 15-17). Por tanto, es posible que la contratación de dichos servicios esté sometida a leyes y tribunales de terceros países con estándares y niveles de protección al consumidor no equivalentes a aquellos previstos por la UE (ya sea en regulación tradicional o en MiCA). Es por estos motivos por los que el crecimiento de estos servicios no ha sido tan prometedor como en un principio se esperaría.

MiCA viene a establecer seguridad jurídica en las reglas del juego de los proveedores de servicios de custodia de criptoactivos para aquellos casos en el que el activo en custodia esté contemplado en la regulación. Cabe decir que ciertos tipos de fichas no fungibles, fichas catalogadas como dinero electrónico o *tokens* catalogados como instrumento financiero bajo MiFID II, no estarán sujetos a estas normas. A las obligaciones genéricas aplicables a los custodios cripto como proveedores de servicios de criptoactivos (CASP) se incorporan previsiones específicas de este tipo de actividad en el artículo 70 de MiCA.

Desde una perspectiva regulatoria, se prevé que exista una relación contractual con los clientes que contemplen detalle de sus obligaciones y responsabilidades, así como determinadas disposiciones obligatorias (identificación de las partes, naturaleza del servicio, ley aplicable, comisiones, medidas de seguridad, canales de comunicación). También se requiere que este tipo de CASP cumpla con ciertos requisitos, que incluyen: (i) compartir una política de custodia, (ii) proporcionar trimestralmente un extracto integral que muestre los balances, las posiciones y los movimientos, (iii) tener implementado un proceso de devolución de los criptoactivos en custodia, así como su compensación en caso de que no sea posible la devolución, (iv) contar con una adecuada segregación de activos de los clientes.

Además, se contempla un régimen de responsabilidad, puesto que los custodios deben ser responsables de cualquier daño producto de un incidente relacionado con las fallas tecnológicas (ciberataques o fallos en la programación del código)<sup>125</sup> (considerando 83 del MiCA). Debido a que en la redacción inicial del MiCA no existía ningún tipo de especificación, dicho régimen se entendió como demasiado amplio o estricto, no siendo equivalente al que existía para el supuesto de la custodia de activos tradicionales y

---

<sup>125</sup> “Es necesario que dichos proveedores de servicios de criptoactivos sean responsables de todo daño que se produzca a raíz de un incidente relacionado con las tecnologías de la información y las comunicaciones (TIC), incluidos los incidentes derivados de ciberataques, robos o cualquier tipo de disfunción.”

resultando en una potencial huida o rechazo de la oferta de este tipo de servicios en la UE.

Por este motivo, la versión final publicada en 2023 especificó que dicha responsabilidad se atribuirá siempre y cuando esté relacionada con la prestación del servicio y la operativa del proveedor. También se aclaró que la responsabilidad tendrá un límite del valor de mercado de los criptoactivos perdidos. Todo esto permite inferir que la custodia de criptoactivos es un elemento esencial para su adopción (especialmente por clientes de alto poder adquisitivo, clientes institucionales, banca tradicional y fondos). Su rol se hace aún más crítico debido a que estos proveedores también podrán encargarse de la custodia de los activos garantizados para la emisión de criptomonedas estables (artículo 37 de MiCA). Por esta razón, será necesario ver su evolución a lo largo de los próximos años.

## **4.2 Servicios adyacentes**

Existen ciertos servicios que se han desarrollado y que se pueden catalogar como subsidiarios o subyacentes, como los seguros específicos del mundo DeFi, los facilitadores de interoperabilidad o los agregadores de visualización, los cuales se analizan a continuación.

### **4.2.1 Seguros**

Los seguros en entornos DeFi se encuentran enfocados en la actualidad a la cobertura de fondos en casos de hackeos de las billeteras, ataques a los protocolos o la existencia de los denominados *bugs* o errores en los contratos inteligentes (Wharton School, Digital Asset Project, World Economic Forum, 2020, pp. 1-20), así como ante casos de *Stablecoin default* (casos en los que la criptomoneda estable cae por debajo de los valores de referencia), o pérdida de las claves privadas de acceso a billeteras cripto (McKinney, 2020, p. 99). Más recientemente han comenzado a aparecer opciones de agrupación de coberturas adaptadas a los usuarios.

En la actualidad, se trata de un nicho aún por desarrollar, con escasez de plataformas enfocadas a este tipo de soluciones (principalmente Nexus Mutual, Opium Insurance e InsurAce Protocol). Además, las coberturas no se dan para todo tipo de protocolos o de *Blockchain*, por lo que su limitación en oferta de productos es aún mayor.

Aún no han aparecido figuras de reaseguros equivalentes a los roles que existen en el mundo centralizado, pero cabe la posibilidad de que estos modelos se desarrollen en una etapa de madurez posterior del vertical asegurador. Este sector, por tanto, se encuentra aún lejos de su potencial uso masivo para cobertura de productos y servicios del día a día (actualmente solo se centran en las problemáticas surgidas de la operativa propia del entorno descentralizado). Por este motivo, sus casos de uso se encuentran aún muy alejados de un potencial uso con finalidades de inclusión financiera o necesidades del mundo fuera de la cadena de bloques.

Sin embargo, una futura expansión de la oferta de servicios hacia necesidades más tangibles podría tener efectos beneficiosos en términos de reducción de costos para los asegurados debido a la reducción de procesos manuales y automatización de decisiones. Otra de las principales ventajas previstas sería la reducción de tiempos en caso de pérdida efectiva o de darse el evento objeto de la cobertura.

Los precios de este tipo de seguros variarán en función de varios elementos como (i) la cantidad y periodo de cobertura deseados y (ii) las características del contrato inteligente que sea objeto de cobertura. Respecto a su operativa, similar a los casos antes vistos, la liquidez en los casos de seguros suele proveerse mediante el depósito de colateral a cambio de las fichas propias del protocolo, a través del cual reciben intereses (Caballero et al., 2020, p. 357).

En estos modelos pueden existir distintos roles (por ejemplo, asesores en los procesos de reclamación o asesores de riesgos, como Nexus Mutual). La Figura 41 muestra una comparativa a alto nivel entre los esquemas operativos tradicionales frente a la operativa de seguros DeFi.

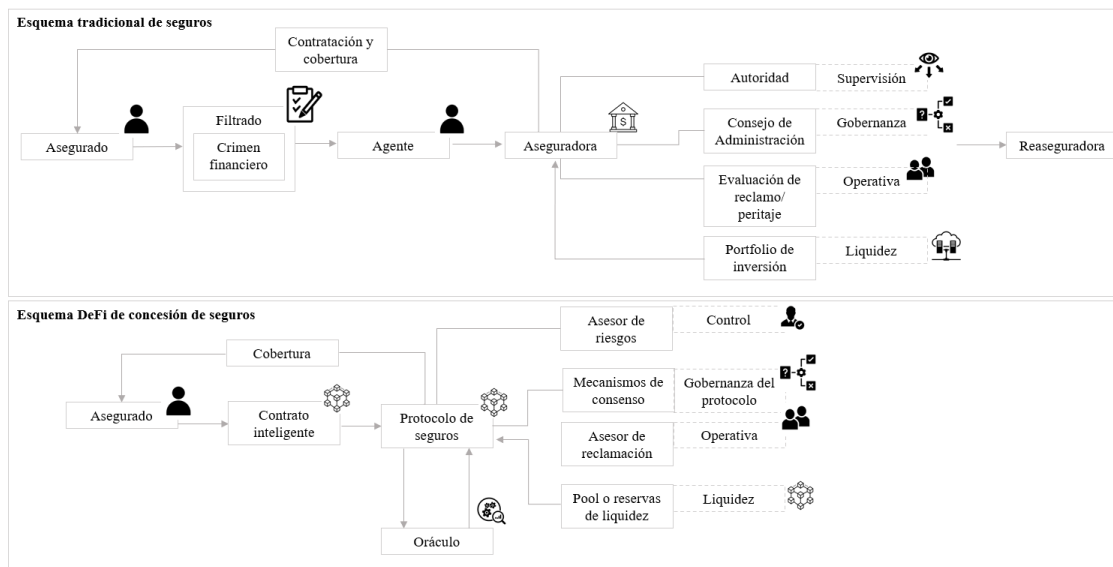


Figura 41. Comparativa de los esquemas tradicionales de seguros frente a esquemas DeFi

Nota. Elaboración propia.

Los asesores de riesgos realizan apuestas de valor sobre los contratos inteligentes objeto de la cobertura, de tal manera que garantizan que dicho contrato es fiable. Para ello, el asesor de riesgos debe contar con la capacidad de asesoramiento del riesgo objeto del contrato de seguro o debe delegar a un tercero esta capacidad (Lau et al., 2020, p. 136). Los eventos de reclamaciones pueden resolverse de dos formas: por medio de terceros verificadores (oráculos) o verificaciones a través de determinados miembros de la comunidad (los asesores de procesos de reclamación, si se habla de Nexus Mutual) (Karp y Melbardis, 2021, pp. 1-16).

A modo de ejemplo, en el supuesto de Nexus, los asesores de procesos votan si aprueban o deniegan el caso, requiriendo un consenso del 70 % de estos. Durante el periodo de votación, los participantes bloquean sus *tokens* y no pueden votar durante las 12 horas siguientes respecto a cualquier otro caso que se produzca. En caso de no alcanzar el porcentaje requerido, la votación se amplía a todos los miembros, requiriendo esta vez una mayoría simple (Karp y Melbardis, 2021, pp. 1-16). La cuestión que podría plantearse en estos casos sería que estos modelos necesitan una distribución amplia de las fichas para evitar concentraciones en la capacidad de toma de decisiones.

#### 4.2.2 Facilitadores de interoperabilidad

Los facilitadores de interoperabilidad de DeFi son soluciones multicadena que permiten la compatibilidad entre distintas *Blockchain* existentes que operan bajo acuerdos

de consenso dispares entre sí. De hecho, facilitan la interoperabilidad entre protocolos abiertos y cerrados (Wood, 2016, p. 1-21).

Existen dos tipos de soluciones diferentes para remediar las barreras de interoperabilidad. La primera es la de mensajería entre cadenas (*cross chain messaging*), a través de la cual se comparte información o mensajes del estado de una *Blockchain* con otra. La segunda permite el intercambio atómico de fichas (*cross chain atomic swaps*), prescindiendo de la intervención de terceros (Hammer, 2021). Este tipo de protocolos no solo ofrecen una opción de mejora de la interoperabilidad entre las distintas redes, sino que también suponen una propuesta de avance respecto a problemas de escalabilidad y capacidad de las que en la actualidad adolecen las *Blockchain* (Wood, 2016, p. 1-21).

Estas soluciones representan tanto un reemplazo de las cadenas originales o sus criptoactivos, como también una operativa similar a un servicio de aduanas o un puente para pasar de una cadena a otra. En casos como el de Polkadot, existen figuras de control de las operaciones, tales como validadores y nominadores. A su vez, en este caso en concreto, existen figuras que monitorizan el correcto comportamiento de los validadores y tienen capacidad de escalado de comportamientos inadecuados (a esta especie de auditor se le denomina *fisherman* o pescador) (Wood, 2016, pp. 1-21).

Sin embargo, estos puentes entre *Blockchain* lo han empleado con frecuencia organizaciones criminales para ocultar o impedir la trazabilidad de fondos ilícitos, puesto que los facilitadores de interoperabilidad permiten el movimiento de fondos a varias cadenas, pudiendo ser cadenas menos conocidas que no cuentan con la cobertura o monitorización adecuada. Es decir, se emplean estas soluciones para fraccionar los fondos en distintas *Blockchain*, siendo varias de ellas de menor categoría y, por tanto, no cubiertas por soluciones *Blockchain* de crimen financiero.

Otro de los riesgos abiertos en estos facilitadores es el de ciberseguridad o *hackeo*, siendo uno de los casos más conocidos el suceso del puente Horizon de Harmony, víctima de un ataque de alrededor de 100 millones de dólares (Neward, 2022, pp. 1-8).

## **5. Nuevos servicios nativos del mundo cripto: oráculos**

### **5.1 Concepto y tipos**

Los oráculos son una herramienta empleada para resolver problemas relacionados con la necesidad de verificación de elementos o eventos que suceden en el mundo real (por

ejemplo, comprobación del precio del activo subyacente). Esto se debe a que, en ocasiones, los contratos inteligentes requieren de condiciones o elementos que suceden fuera de la *Blockchain*. En estos casos, los oráculos funcionan como un nexo que transforma la información de tal forma que pueda ser procesada y chequeada por los protocolos que operan en tecnologías de registros distribuidos.

Como tal, esta figura no existe en el mundo de las finanzas tradicionales debido a que ya operan en el mundo real. Tampoco es una figura contemplada en el MiCA pese a ser un foco de riesgo y debería de ser evaluada como potencial actividad sujeta a una nueva normativa, motivo por el cual se analizará esta figura en mayor detalle y se expondrán cuáles son las principales debilidades que en la actualidad no se están atendiendo.

Los oráculos pueden clasificarse en función de distintos criterios, tales como la forma de obtención de datos, su función, la dirección de los flujos de información o comprobación, su uso, cómo se integran, su forma de validar la veracidad de la información o el nivel de descentralización de la organización gestora del oráculo. La taxonomía de uso más habitual es en función de su origen, la cual se desarrolla a continuación:

Primeramente, se podría hablar de los denominados oráculos humanos, que son aquellos que se emplean cuando los contratos inteligentes requieren la verificación a través de medios humanos, como pueden ser notarios o autoridades.

Un segundo tipo son los oráculos *hardware*. Bajo este concepto se identifican aquellas soluciones que se utilizan cuando los *smart contracts* requieren la validación principalmente mediante el empleo de medios relacionados con el IoT, como geolocalizadores, códigos QR o de barras, sensores, entre otros. Este tipo de oráculos cuenta con gran potencial de uso en casos de importación y exportación, en los que la llegada de barcos o movimientos de contenedores puede desencadenar la orden de pago en el contrato inteligente.

Un tercer tipo son los oráculos *software*, que son aquellos que se manejan cuando los contratos inteligentes requieren la validación de elementos disponibles en formato digital, ya sea mediante la conexión API, información disponible en web cuya captura es posible a través de uso de programas u otros medios. Este tipo de oráculos se ha planteado como una posible solución a la necesidad de incluir medidas de prevención de blanqueo en las operaciones descentralizadas. A través de los oráculos de prevención de blanqueo y



financiación del terrorismo, la operativa podrá verificarse contra listas de riesgo, incluyendo direcciones cripto de alto riesgo.

A continuación, en la Figura 42 se expone un ejemplo de la operativa de oráculos descentralizados (puede funcionar en ambos sentidos: de la *Blockchain* hacia el mundo real y viceversa).

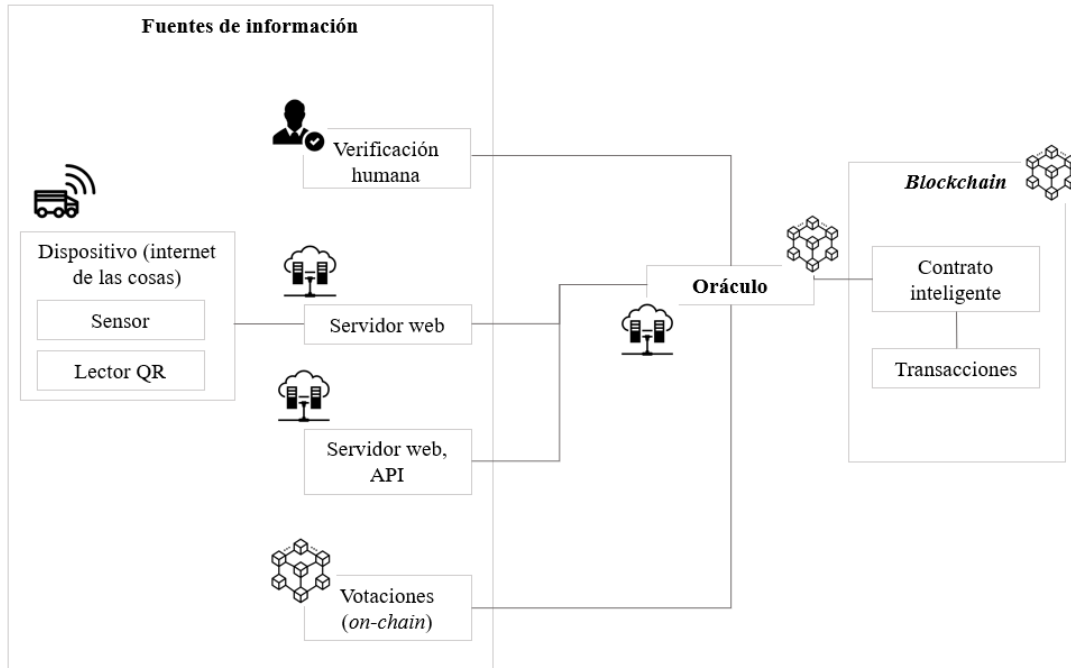


Figura 42. Ejemplo de la operativa de un oráculo

Nota. Elaboración propia.

Como se observa en la Figura 42, existen distintas fuentes de información: humanas, de *hardware*, digitales o incluso en la cadena. Estas fuentes de información son capturadas por los oráculos y estos, a su vez, sirven de punto de conexión o referencia de los contratos inteligentes en la *Blockchain*.

## 5.2 Casos de uso

Los oráculos han ido creciendo en su utilidad a lo largo del tiempo, y se espera que su potencial siga aumentando en proporción a los nuevos productos y servicios que se generan dentro de las DeFi.

El caso de uso más destacado relacionado con las criptodivisas son las *stablecoins* y los activos sintéticos, puesto que requieren conocer el tipo de cambio entre el activo del mundo real y el activo en *Blockchain* (Eskandari et al., 2021, p. 2). En cuanto a los casos

de uso transaccionales, generalmente están relacionados con la necesidad de conocer precios de los activos, como derivados, mercados predictivos, casas de cambio y proveedores de liquidez descentralizados, entre otros (Eskandari et al., 2021, p. 2). Un tercer caso de uso es el relacionado con el establecimiento de los controles en DeFi mediante los oráculos de verificación de identidad (Eskandari et al., 2021, p. 2) o los chequeos contra listas, como se mencionó anteriormente.

### ***5.3 Problemáticas que plantean***

Como se ha podido deducir, los oráculos están operando como una fuente única de la verdad para numerosos protocolos DeFi. Por lo general, suelen ser interoperables, por lo que se emplean en varias *Blockchain*, no exclusivamente en Ethereum. Esta dependencia de numerosos protocolos en distintas cadenas en paralelo genera el riesgo de concentración en un único punto de fallo en caso de que los oráculos adolezcan de errores en el código de programación o sean atacados, pudiendo generar contagios masivos en escenarios de oráculos de precios, por ejemplo.

En la actualidad, el uso de los oráculos puede no ser material, pero su potencial de crecimiento es grande. Por ese motivo, desfases en la provisión de información (latencia) debido a la falta de capacidad de respuesta del oráculo ante numerosas solicitudes de verificación podría generar alteraciones en los precios de los protocolos que operan con ellos (Kaleem y Shi, 2021, pp. 7-8). Además, al igual que en otros casos, surge la pregunta de quién verifica al verificador, puesto que los oráculos no están sujetos a obligaciones de auditorías tecnológicas. De hecho, los supervisores globales han comenzado a discutir cómo crear ambientes de control en las DeFi, pero estos siempre se han enfocado principalmente en los proveedores de servicios de criptoactivos o emisores de criptoactivos, pero no en los oráculos, dado que sus servicios se consideran accesorios.

Con respecto a la interacción de los actores regulados centralizados con los oráculos DeFi, esta relación puede no ser material en este momento, pero en el futuro es probable que los proveedores de servicios de criptoactivos descentralizados se convertirán en partes reguladas (mediante licencia o registro según la región). En ese punto, la interacción con oráculos y la debida diligencia sobre estos se convertirá en un tema a abordar. Bajo el supuesto de que algunos de ellos se considerarán como proveedores de servicios críticos o materiales, es posible que sea necesario considerar la analogía con la futura ley de resiliencia operativa digital (DORA), teniendo en cuenta la aplicación de

dos principios clave que se desarrollarán más adelante: el principio de proporcionalidad y el principio de un enfoque basado en el riesgo.

La implementación de una carga regulatoria demasiado pesada puede resultar en la falta de un oráculo que se ajuste a todos los requisitos. En contraste, tratar a los oráculos como otro proveedor no abordaría adecuadamente el riesgo que plantean, lo que tiene implicaciones en los servicios financieros ofrecidos. En consecuencia, un equilibrio adecuado entre el riesgo y los controles debe sustentar la relación entre los protocolos y los oráculos.

Cabe concluir que existe un riesgo latente en los oráculos a medida que aumenta su uso y, por tanto, la dependencia en ellos. La posición de que esta actividad ha de ser regulada se sustenta en base a que los oráculos son actualmente fuente de información para la provisión de precios de las criptomonedas estables, que ya están contempladas en MiCA debido a su amplia acogida por el público en general. La dependencia crítica de las criptomonedas estables en los oráculos hace que se consideren equivalentes a proveedores de servicios críticos en el Reglamento DORA que se trata en la segunda parte de la tesis.

## **VI. EL ROL DE LA BANCA INSTITUCIONAL EN *FINTECH* 4.0**

Los participantes en las finanzas tradicionales también juegan un papel en *FinTech* 4.0. Para la banca tradicional (especialmente la banca institucional y de inversión), los criptoactivos y los mercados descentralizados amplían la oferta de servicios financieros debido a la generación de nuevas categorías de activos que pueden generar negocio, especialmente debido al interés mostrado no solo por los clientes personas físicas, sino también por los clientes personas jurídicas.

Además, el uso de la tecnología subyacente se considera una forma de mejorar la eficiencia de costos operativos y de contratación, lo que mejora la cuenta de resultados de estas entidades mediante la aplicación de innovación tecnológica. Por ejemplo, Ibáñez (2018) mencionó el potencial del uso de un *scoring* de crédito y solvencia basado en *Blockchain*, que podría ajustar el crédito en función de los pagos sin necesidad de intervención humana (Ibáñez, 2018, pp. 164-165). De hecho, se ha ido evidenciando un aumento de la participación institucional, alcanzando altos volúmenes de operaciones en las principales cadenas, tal y como se observa en la Figura 43 (Chainalysis, 2022, p. 11).

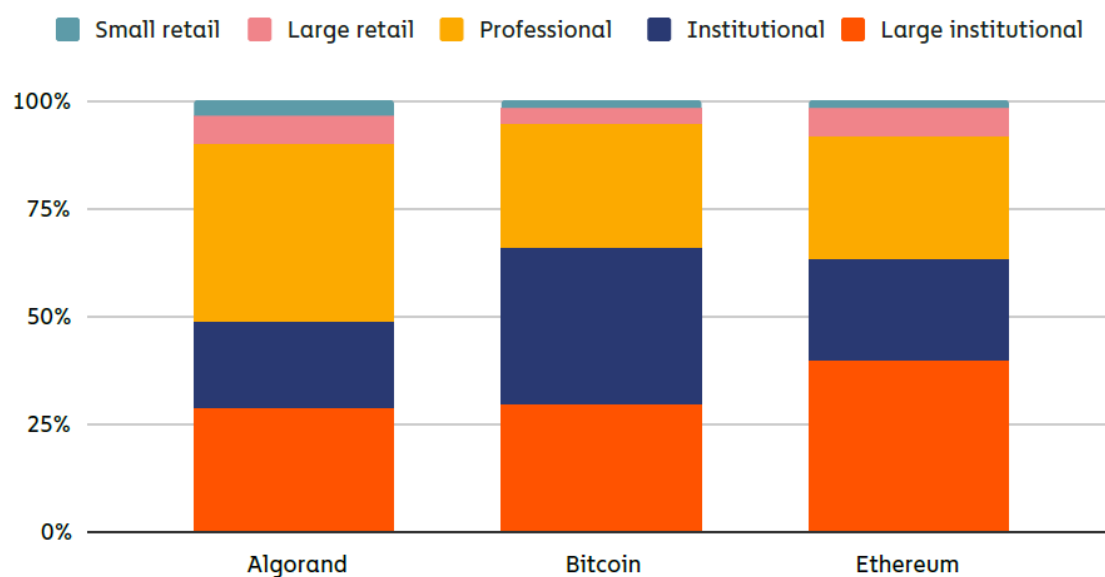


Figura 43. Volumen de transacciones por categoría de tamaño de transferencia, junio de 2021 a mayo de 2022, Algorand, Bitcoin y Ethereum

Nota. Tomado de *The Chainalysis state of Web 3.0 report*, por Chainalysis, 2022, <https://go.chainalysis.com/2022-web3-report.html>.

La Figura 43 muestra el volumen de transacciones de junio a mayo de 2022 en Algorand, Bitcoin y Ethereum. *Small retail* son transacciones por debajo de 1000 USD, *large retail* entre 1000 y 10 000 USD, *professional* entre 10 000 y 1 000 000 USD, *institutional* entre 1 000 000 y 10 000 000 USD y *large institutional* por encima de 10 000 000 USD. Como se puede observar, las grandes instituciones, instituciones y profesionales copan la enorme mayoría de las transacciones de criptoactivos en las *Blockchain* de Bitcoin, Ethereum y Algorand. Los tramos de grandes instituciones, instituciones y profesionales acumulan más del 75 % de los volúmenes totales de transacciones.

Sin embargo, los participantes tradicionales se enfrentan a diversos retos de carácter legal, cultural y técnico. Desde el punto de vista legal o regulatorio, las instituciones financieras son entidades altamente reguladas y supervisadas, que han experimentado las implicaciones de incumplimientos o el no alcanzar las expectativas regulatorias. Por tanto, parten de una situación de carga moral y regulatoria producto de años de interacción con el supervisor. Este elemento hace que adopten una posición conservadora o de espera hasta que se alcance un terreno de certidumbre externa (regulación, guías supervisoras) que permita vislumbrar los márgenes para operar de forma segura. Además, desde el punto de vista prudencial, el Comité de Basilea publicó en diciembre de 2022 un informe

con los criterios básicos de tratamiento de la exposición a criptoactivos por parte de la banca, clasificando los criptoactivos desde el punto de vista prudencial y desincentivando la exposición a aquellos de mayor volatilidad a través de exigencias en los ratios de capital.

Del primer reto se deduce el segundo, es decir, los retos culturales. Como se mencionó anteriormente, la experiencia vivida hace que las entidades financieras tradicionales tiendan a tomar posiciones reactivas o de espera ante las innovaciones *FinTech* y los nuevos mercados. Además, los volúmenes manejados aún no pueden considerarse lo suficientemente representativos como para tomar decisiones de gestión basados en elementos cuantitativos. Solo aquellas entidades financieras que sopesan ingredientes cualitativos como el potencial futuro de la implantación temprana de la nueva tecnología se aventuran a desarrollar sus propias soluciones de experimentación.

Finalmente, los elementos técnicos presentan un reto a las entidades financieras, puesto que requieren un mapeo y adaptación de un gran número de elementos para poder llevar a cabo integraciones adecuadas. A modo de ejemplo, en las TradFi, las acciones son completas; sin embargo, en el mundo cripto, se dan casos de fracciones de hasta ocho dígitos tras el separador. Además, los cambios tecnológicos tienen implicaciones que requieren de decisiones tanto operacionales (cómo trabajar en mercados globales en los que se puede operar en 24 horas durante todo el año) como estratégicas (consideraciones de concentración de la exposición a criptoactivos).

Dentro de esta última categoría se pueden englobar las problemáticas de integración con CASP y su elección, regulados tanto dentro del MiCA como dentro de la Directiva de Prevención de Blanqueo, la normativa del denominado “*travel rule*” y en DORA<sup>126</sup>. El nuevo proveedor de servicios deberá adecuarse no solo desde el punto de vista tecnológico, sino también desde el regulatorio, por lo que es de esperar que las instituciones financieras extiendan sus requerimientos regulatorios y de cumplimiento a los proveedores de servicios de criptoactivos (*crypto assets service provider*) o CASP, especialmente en lo que respecta al crimen financiero, protección de datos, abuso de mercado, conflictos de interés, transparencia y protección a los inversores.

Debido a que no todos los CASP pueden catalogarse como aptos para estos estándares, podría darse *de facto* la situación de concentración de proveedores de servicios de

---

<sup>126</sup> Estas normativas y propuestas son objeto de análisis crítico más adelante.

criptoactivos para la banca tradicional y sus clientes. Sin embargo, en la actualidad, MiCA no contempla controles especiales para este tipo de proveedores que podrían llegar a verse como sistémicos del mundo cripto, a diferencia de lo que sucede con los emisores. Por esta razón, sería recomendable contemplar la posibilidad de distintos niveles de CASP y, consecuentemente, distintos niveles de controles y responsabilidades a asignárseles, siguiendo los principios de proporcionalidad y enfoque basado en riesgos.

Desde el punto de vista estratégico, las entidades financieras, especialmente aquellas que ofrecen una banca universal con todo tipo de productos y servicios, deben establecer cuál va a ser su punto de entrada o incursión en el mundo cripto, siendo, por lo general, su pilar la introducción de servicios de custodia de criptoactivos (Reul et al., 2022).

## **VII. RETOS: ENFOQUE BASADO EN RIESGOS Y PROPORCIONALIDAD APLICADOS A POLÍTICAS REGULATORIAS**

En efecto, los desarrollos normativos de la zona euro en la actualidad se centran en los criptoactivos y la provisión de servicios relacionados que son ofrecidos por entidades con cuerpo jurídico. La regulación existente se enfoca en la prevención de crímenes financieros. Por su lado el Reglamento MiCA abarca elementos de protección al consumidor y transparencia, pero aparentemente no se aplicaría a DeFi y sus nuevas actividades o figuras.

El MiCA requerirá normas técnicas de desarrollo en diversos ámbitos (regulación, ejecución y actos delegados). A modo de ejemplo, los formatos específicos de los libros blancos (arts. 6, 19 y 51 de MiCA) o los formularios de intercambio de información entre autoridades se harán públicos a través de estos instrumentos. En el momento en que se publique la normativa de desarrollo (segundo y tercer nivel), es muy probable que hayan surgido aún más servicios descentralizados que se encuentren fuera del alcance de la supervisión y que se hayan añadido a los existentes en 2023, cuando MiCA se acababa de publicar.

Por ese motivo, es necesario el rediseño de los procesos normativos y de supervisión, requiriendo de entornos normativos basados en principios que puedan ser objeto de desarrollo a través de guías del propio supervisor. El control tradicional sobre entidades centralizadas que operen o tengan como objetivo los consumidores europeos es posible; sin embargo, los casos en los que no existe un ente jurídico o una persona física identificada o identificable cada vez son más en DeFi, abriendo la discusión sobre cómo

se han de regular este tipo de actividades. Incluso, los decisores (dueños de las fichas) pueden llegar a ser miles y estar distribuidos en todo el mundo. Esto hace que los esfuerzos por supervisar y controlar este tipo de operaciones como se ha venido haciendo hasta ahora resulten excesivos y sumamente ineficaces en términos de coste, esfuerzo y resultados.

Por tanto, en lo que respecta a las DeFi, coincidiendo con la postura de Auer, parte de las soluciones propuestas en esta tesis es que se deberían buscar soluciones que estén diseñadas o incrustadas dentro de las propias cadenas o protocolos (Auer, 2019, pp. 1-31), similar al principio de protección de datos por diseño establecido en la regulación europea de protección de datos, de manera que los formatos como los ERC en *Ethereum* incorporen requisitos de comprobación sobre ciertos elementos hasta ahora no relacionados con cumplimiento o normativas. Asimismo, los controles deberían ser proporcionales a la materialidad de las actividades ofertadas por los protocolos, siguiendo un enfoque basado en riesgos con el fin de centrar esfuerzos de supervisión en aquellas plataformas o servicios que se consideren materialmente relevantes.

Dado que las cadenas y protocolos son globales y pueden ser operados por entidades o personas de diversos países, surge la necesidad de contar con una figura de coordinación de supervisores que tenga la capacidad de llegar a acuerdos mínimos a ser aplicados por los reguladores y supervisores nacionales, similar a la solución ya adelantada en el capítulo de *FinTech 3.0 – 3.5*. Esta entidad tendría como funciones principales establecer estándares o guías de supervisión holísticos para las DeFi y las criptomonedas, coordinarse con instituciones internacionales como IOSCO, Basilea o FATF, y supervisar los acuerdos sistémicos o globales de *stablecoin arrangements* sistémicos o globales en términos de volúmenes mundiales o deslocalización de órganos decisores.

Este tipo de entidad diseñaría estándares o recomendaciones que se convertirían en estándares mínimos a nivel global, y que serían puntos de partida para los desarrollos normativos a nivel regional o local. Bajo este prisma, podrían diseñarse plataformas de macrosupervisión de los mercados para detectar señales de alerta y evitar inestabilidades globales como, por ejemplo, fugas masivas de capitales o riesgos de falta de liquidez inminente. También podría ser capaz de asesorar el riesgo del total del ecosistema DeFi y exigir refuerzos en las partes que conforman la cadena, ya sea en aspectos contractuales, de fraude o cualquier otro. De esa manera, el riesgo de la limitación en el asesoramiento

integral de los riesgos por parte de los supervisores locales (G7 Working Group on Stablecoins, 2019, pp. 7-27) se superaría a través de este punto común de concentración.

Esta propuesta requiere mayor integración y podría plantear cuestiones de cesión de soberanía; sin embargo, debido al carácter global de las DeFi, podría ser una solución comprensiva y eficaz. A su vez, debido al nuevo planteamiento tanto de las finanzas como de la interacción con los supervisores, será necesaria la apertura al diálogo público-privado. Por consiguiente, herramientas como la supervisión integrada, las monitorizaciones en tiempo real y el diseño de unidades de supervisión especializadas (Comisión Europea, 2020c, p. 1), con conocimientos técnicos y apertura al cambio, serán necesarios a lo largo de los próximos años.

A grandes rasgos, las DeFi plantean grandes retos normativos que se benefician de acuerdos globales coordinados en los siguientes aspectos: el (i) control interno, (ii) las estructuras e incentivos de gobernanza, (iii) el régimen de responsabilidad, (iv) la resolución de conflictos y protección a los consumidores, (v) el balance entre privacidad y crimen financiero, (vi) la ciberseguridad y (vii) la necesidad de aumentar el número de especialistas en tecnoderecho por parte de los organismos públicos.

## **VIII. METAVERSOS. LA NECESIDAD DE MARCOS NORMATIVOS PROPIOS**

El metaverso se define como un “entorno virtual, en línea, en el que las personas pueden comunicarse, relacionarse, jugar y trabajar. Es el siguiente nivel de internet, pero más intensivo, integrado e inmersivo” (Écija, 2022, p. 4). La acepción apareció por primera vez en 1992 en la novela *Snow crash* de Neal Stephenson. Ideas similares a las de la necesidad de monedas virtuales se ven reflejadas en su novela *Criptonomición* de 1999. La palabra en sí cuenta con dos raíces: *meta* (más allá) y *verso* (universo). Pese a que el término es generalmente empleado en singular, en realidad no existe un único metaverso, sino varios (es decir, hay metaversos o multiversos, no un metaverso).

Las evoluciones de internet de la Web 2.0 hacia la Web 3.0 han permitido que las interacciones entre usuarios que ya venían dándose en videojuegos progresen hacia un entorno de realidad virtual o realidad aumentada, en el que los jugadores pueden ver, escribir y modificar. Son dueños de los datos y de sus interrelaciones, e incluso tienen la capacidad de replicar objetos de la vida real en el mundo virtual, llegando a alterarlos o mejorarlos a su gusto. Al respecto, Serrano señaló:



*[...] nos encontraríamos ante un Internet ciberfísico y potenciado por la tecnología, capaz de superar el paradigma del Internet móvil convirtiéndose en el siguiente salto evolutivo de nuestras capacidades de interconexión física y digital, y, por tanto, también de nuestra vida social.*

*En definitiva, nos encontraríamos frente a un salto desde la bidimensionalidad de los sitios web insertos en pantallas cuadradas hacia la tridimensionalidad esférica de lo espacial y hacia la cuatrimimensionalidad de los sentidos (...), siendo difícil, llegados a ese punto, discernir entre la “realidad real” y la “realidad virtual”. (Serrano, 2022, p. 94)*

Tal y como se puede desprender de las definiciones previamente expuestas, los metaversos cuentan con ciertos elementos que los caracterizan, entre los cuales se incluyen: (i) la capacidad de interactuar libremente entre los usuarios, (ii) la sensación de inmersión en el mundo virtual o la alteración del mundo real a través de técnicas de realidad aumentada, (iii) la capacidad de interoperar independientemente de un juego o una plataforma, lo que potencialmente permite que un personaje, objeto o premio creado en un juego pueda trasladarse a otro entorno (ya sea un juego, una plataforma o incluso un lugar virtual de reuniones), (iv) la inmutabilidad y durabilidad, ya que no existen límites de tiempo o “apagado”. Estos aspectos han planteado problemáticas jurídicas, como qué sucede con los avatares que permanecen en los metaversos más allá de la vida de sus propios usuarios.

Los metaversos han logrado desarrollar no solo ambientes de juegos, sino también entornos de negocios y educacionales, lo que ha despertado el interés de numerosas multinacionales e incluso actores públicos que han comenzado a mostrar su presencia en los metaversos. De esa manera, se está creando un mundo virtual en el que los aspectos lúdicos se mezclan con asuntos más serios, como la compra de inmuebles o la contratación de productos financieros.

Estos nuevos universos aumentados tienen sus propias organizaciones basadas en principios de descentralización, que son las DAO, como se analizó previamente. También cuentan con sus propias finanzas y activos, que se reflejan en DeFi, criptoactivos y NFT, como una forma de representar la propiedad en los metaversos. Por esta razón, los metaversos funcionan como un estrato en el que convergen las DeFi, las organizaciones

propias de este universo y sus propias divisas. Por lo tanto, se deduce que su crecimiento y adopción estarán vinculados a estos componentes.

En ese orden de ideas, la intención del empleo de criptodivisas no es otra que la de incentivar la interoperabilidad entre plataformas y negocios del metaverso, permitiendo su utilización de forma transversal en los metaversos y evitando que su uso se quede limitado a un juego o una aplicación (Serrano, 2022, p. 109). Similar a las problemáticas jurídicas ya expuestas en las DAO, criptoactivos y DeFi, los metaversos plantean grandes retos, siendo el primero de ellos cuál es la jurisdicción, la regulación, la supervisión y los tribunales aplicables a un universo virtual que nace con un carácter global.

Al igual que en los casos anteriores, la posición de esta tesis es que, debido a que se está ante un fenómeno radicalmente distinto a lo anteriormente conocido, en los cuales DeFi y los criptoactivos serían elementos esenciales, pero solo parte de un panorama más amplio. De este modo, DeFi y los criptoactivos requerirían de marcos normativos y de supervisión en el ámbito financiero, mientras que cuestiones relacionadas con el derecho civil, la propiedad intelectual e industrial e incluso el derecho penal deberían establecer sus propias especificaciones con respecto a las actividades desarrolladas en los metaversos.

## **IX. PRINCIPALES MENSAJES**

El concepto de *confianza* no desaparece en las DeFi, sino que se transforma. Se pasa de confiar en un tercero financiero (banco central o entidad financiera) a un tercero tecnológico localizado en cualquier parte del mundo (el desarrollador o programador del criptoactivo, *smart contracts* o los protocolos). Por este motivo, el derecho y la supervisión financiera necesitan progresar, al menos en este espacio, hacia el tecnoderecho y la tecnosupervisión. Además, estos nuevos terceros de confianza deben tomar conciencia de su nuevo rol y las implicaciones que tiene para el mercado, lo cual requiere el desarrollo de soluciones de autocontrol. Desde el prisma del enfoque regulador y supervisor, este tendría que atravesar tres fases principales: comprensión, estrategia y ejecución.

La fase inicial de comprensión abarcaría el entendimiento del universo descentralizado, identificando su potencial y riesgos. Este primer paso no puede llevarse a cabo de forma unilateral, sino que es necesario un diálogo constructivo público-privado. Además, la comprensión requerirá un cambio en los perfiles y la filosofía de supervisión.

Herramientas similares a los *sandbox* regulatorios podrían contribuir a una primera aproximación entre ambos sectores para un intercambio de expectativas, así como una posible forma de alcanzar soluciones constructivas. Este estadio tendría que ser dinámico y continuo en línea con cómo se está comportando este sector en cambio constante.

Esta etapa de exploración deberá abarcar no solo a los actores emergentes y su nivel de madurez en la industria, sino también cuál es el papel de la banca e instituciones tradicionales y su estrategia futura en torno a estos nuevos mundos digitales. Un mejor entendimiento de la evolución del mercado permitirá asesorar de manera dinámica sobre qué servicios se encuentran dentro del ámbito de supervisión en materia financiera. Esto es especialmente relevante en casos híbridos donde se combina una propuesta de valor que abarca tanto servicios financieros como no financieros, o cuando no existe claridad sobre el tratamiento jurídico del producto.

En cuanto al segundo estadio (estrategia), se reconoce que los procesos normativos y de supervisión actuales no se están adaptando al ritmo que requiere DeFi, incluso quedando rezagados desde el momento en que eran borradores. Por lo tanto, es necesario buscar alternativas más flexibles y acordes con los tiempos, como panoramas normativos generales y abiertos basados en principios, que permitan desarrollos técnicos posteriores en forma de guías o recomendaciones. Sin embargo, se debe abordar la necesidad de reducir los tiempos de aprobación administrativa para la publicación de normas.

Debido al crecimiento acelerado y la velocidad que está tomando el ámbito de los criptoactivos y las DeFi, y considerando su naturaleza heterogénea, se propone la creación de una unidad de supervisión dedicada exclusivamente a estos asuntos.

En lo que concierne a la tercera fase de ejecución, un control sobre las entidades o personas supondría un enfoque limitado, el cual se quedaría desfasado debido al volumen de sujetos obligados del que se podría estar hablando, sus cambios constantes y el hecho de que gran parte de ellos probablemente se encontrarán fuera de la UE (Zetzsche et al., 2020, p. 24). Por ese motivo, se requieren medidas como un organismo coordinador de supervisores, un enfoque proporcional y basado en riesgos, así como un mayor control en la arquitectura y el diseño de los protocolos (cumplimiento por diseño). En ausencia de dicha figura coordinadora, se deben considerar esquemas de reconocimiento de equivalencia global y coordinación a nivel regional (Zetzsche et al., 2020, p. 24).

Por otro lado, el sector privado que desarrolla estas soluciones y promueve DeFi como estandarte de inclusión financiera debe buscar la coherencia entre tal afirmación y el producto que diseñan, gestionan en comunidad o promocionan. Hasta ahora, se han identificado comunicaciones positivas con poca imparcialidad en relación con los riesgos o mecanismos de protección a los consumidores. Dado que el control público avanza por detrás de los nuevos modelos, es imprescindible el autocontrol por parte de los agentes que participan en los modelos de DeFi.

Los agentes DeFi se centran en la seguridad basada en la inmutabilidad de las cadenas de bloques, pero para el público en general, la seguridad es un concepto más amplio que también abarca aspectos jurídicos, los cuales actualmente carecen de atención en este ecosistema. De esta forma, se pueden establecer soluciones normativas y controles desarrollados por la propia industria para proteger a los usuarios, especialmente a aquellos menos sofisticados o pertenecientes a poblaciones vulnerables. En ese sentido, las barreras actuales que impiden que DeFi sea una herramienta de inclusión financiera podrían disminuir, y su potencial podría beneficiar a estos colectivos en aspectos fundamentales, como los pagos.

Será necesario realizar un seguimiento tanto de la expansión de las actividades DeFi como de las acciones de las autoridades durante los próximos años, con el fin de determinar si en el futuro DeFi podrá emplearse como una herramienta segura de inclusión financiera.

Por otro lado, en *FinTech* 4.0 acaba de eclosionar una problemática que ya se venía viendo en *FinTech* 3.0-3.5, esto es, la erosión de soberanía estatal y en concreto, de los bancos centrales. Así la tecnología irrumpe en el sector financiero no sólo en los accesos a las finanzas, sino también en los propios servicios e incluso, en el propio núcleo del mundo financiero, al crear alternativas al dinero. Por este motivo se ha visto la necesidad (nunca contemplada con anterioridad), de establecer marcos regulatorios de gestión de no sólo actividades, sino de activos que pueden clasificarse de potencialmente sustitutivos al euro.

En efecto *FinTech* 4.0 muestra un claro desafío en lo concerniente a soberanía estatal, ya que en concreto las criptomonedas estables emitidas por gigantes tecnológicos podrían impactar en las estrategias de política monetaria no sólo de un país, sino de una región o incluso a nivel mundial. Teniendo en cuenta que la emisión de moneda y control de la

oferta monetaria se lleva a cabo con el fin de alcanzar una adecuada estabilidad de los precios y control del crecimiento económico, queda claro que es necesario entender y controlar la innovación de *FinTech* 4.0.

La forma de abordar esta tarea (vía Reglamentos como se verá en la segunda parte) también muestra una tendencia a la centralización de decisiones materiales clave a nivel europeo, dejando menor libertad de movimientos y decisión a los Estados Miembros. Se entiende que el empleo de este instrumento regulatorio se debe al riesgo de fragmentación que podría tenerse en caso de que los Estados regulasen de forma aislada una materia tan incipiente y novedosa. De ser así, se dificultaría la actividad *FinTech* al crear barreras a la innovación y la libre competencia.

En cuanto a la regulación *FinTech* en sí, la autora considera que no sólo ha de centrarse en buscar una estandarización en la región, sino que también ha de tener en cuenta que la UE está en un sistema de competencia global. Esto quiere decir que, si la normativa Europa no va alineada con la de otras regiones, podría desembocar en una huida de la innovación hacia otras regiones. Por consiguiente, una normativa demasiado estricta puede impactar la capacidad de supervisión efectiva de estas actividades, ya que las empresas operarían desde otras jurisdicciones.

En relación con la anterior conclusión y tal y como se sostiene en esta tesis, la coordinación internacional para la fijación de estándares mínimos es crucial para evitar lagunas regulatorias de una actividad que no entiende de fronteras. Sin embargo, el éxito de esta propuesta es bajo teniendo en cuenta que los países a nivel mundial han tomado posiciones discrepantes respecto al asunto, y existen diferencias en términos de prioridades de la temática, o si se ve como una oportunidad o una amenaza.



## **SEGUNDA PARTE. RETOS DE SUPERVISIÓN Y REGULACIÓN**





## **CAPÍTULO V. SUPERVISIÓN *FINTECH*: LA TEORÍA DEL DESFASE SUPERVISOR**

### **I. LOS MECANISMOS TRADICIONALES DE SUPERVISIÓN**

#### **1. Planteamiento**

La función de los bancos centrales o instituciones equivalentes como reguladores y supervisores deriva de la función de los Estados de proteger adecuadamente a los consumidores y garantizar una adecuada estabilidad de los mercados financieros, incluyendo los sistemas de pagos (específicamente en el caso del BCE). También son responsables de diseñar y ejecutar las políticas monetarias acorde con el contexto en el que los países o regiones se encuentren<sup>127</sup>. Esto requiere un equilibrio adecuado entre el control de las instituciones públicas y la gestión de los riesgos asociados con las operaciones del sector privado, especialmente en el caso de modelos innovadores o novedosos que aún no están sujetos a regulaciones establecidas.

Es importante distinguir entre los dos principales roles de los supervisores en este ámbito: como reguladores, establecen las reglas del juego, incluyendo, entre otras, las de acceso a las actividades reguladas; y como supervisores, ejercen control y supervisión en la práctica, establecen expectativas y toman medidas coercitivas o sancionadoras cuando sea necesario.

A continuación, se analizan los esquemas de gobernanza de la supervisión financiera, seguido por una evaluación de los modelos de regulación y supervisión *FinTech* y los retos a los que se enfrentan. Luego se aborda teoría la del desfase supervisor, identificada en esta investigación. Posteriormente, se discute si los *sandbox* regulatorios pueden considerarse una solución estratégica o simplemente una herramienta complementaria. Por último, se presentan propuestas de marcos regulatorios y de supervisión.

#### **2. La gobernanza de la supervisión financiera**

La supervisión de la industria financiera ha ido aumentando su complejidad a lo largo del tiempo debido principalmente a la globalización de la economía. Si bien en las etapas

---

<sup>127</sup> Versión consolidada del Tratado de Funcionamiento de la Unión Europea PROTOCOLO (No 4) SOBRE LOS ESTATUTOS DEL SISTEMA EUROPEO DE BANCOS CENTRALES Y DEL BANCO CENTRAL EUROPEO. DOC 202 de 7.6.2016.

iniciales (equivalentes a *FinTech* 1.0 y parte de *FinTech* 2.0) el ámbito de decisión y supervisión era puramente local, a medida que la operativa financiera y su impacto excedía los perímetros locales, se hacía necesaria la cooperación internacional, la creación de estándares y, por ende, los organismos regionales o supranacionales.

La Unión Bancaria Europea (UBE) es un claro ejemplo de la reacción ante el impacto de la crisis de 2008 en los mercados europeos que arrastró a la zona euro a un aumento de la deuda pública y a una situación de patente riesgo de la estabilidad financiera (Consejo Europeo, 2022b, pp. 1-8). Ciertamente, se añade una capa a la estructura de supervisión financiera a las de las jurisdicciones locales (en el caso español, el Banco de España, la CNMV y la Dirección General de Seguros y Fondos de Pensiones).

Sin embargo, la UE no es más que una de las contrapartes dentro de una composición aún más amplia y compleja suprarregional o global (ver Figura 44). Por este motivo, a medida que ha ido avanzando el desarrollo en los mercados financieros, se ha producido un aumento de la dificultad de las estructuras de supervisión que requieren una mayor coordinación y presentan retos en términos de tiempos y recursos. Además, se ha avanzado hacia una clara separación de verticales bancarios, de inversión y seguros y planes de pensiones.

A estas arquitecturas de gobernanza se suman otros agentes, como los creadores de estándares en determinadas temáticas o nichos como Financial Action Task Force (FATF) para crimen financiero. Finalmente, otro elemento para tener en cuenta es la necesidad de coordinación con otros supervisores transversales o especializados en una materia, como puede ser el escenario de protección de datos, protección a consumidores, competencia o prevención de blanqueo y financiación del terrorismo.

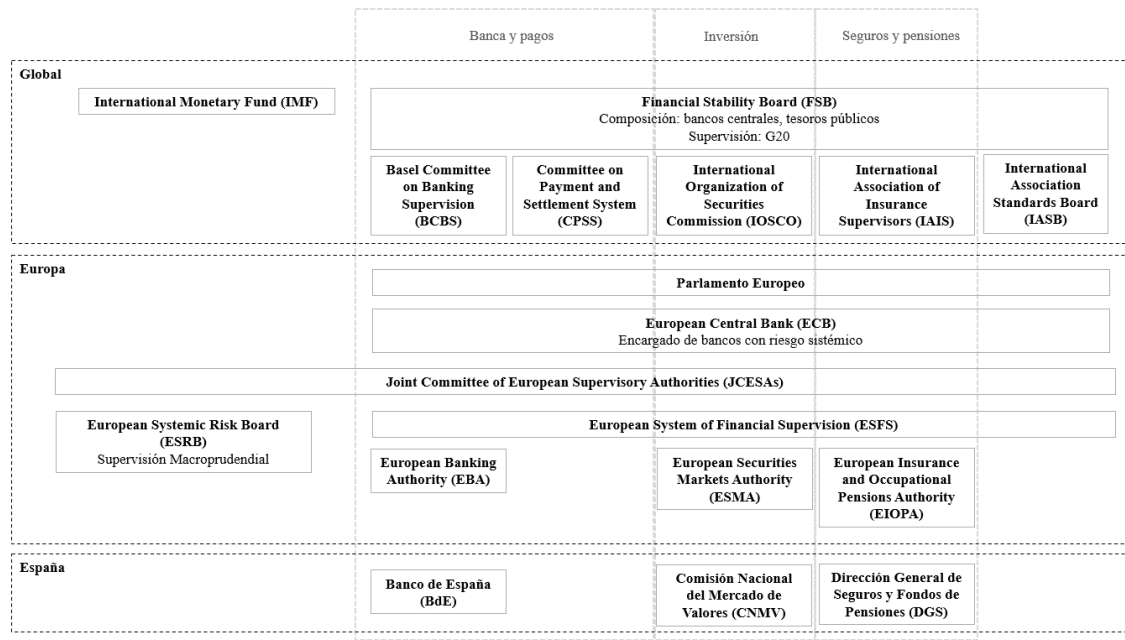


Figura 44. Capas de supervisión por verticales de la industria financiera

Nota. Tomado de *Infografía - EU system of financial supervision*, por Consejo Europeo, 2022a, <https://www.consilium.europa.eu/es/infographics/financial-supervision-architecture/>

Como se advierte en la Figura, tomando el ejemplo de España, existen tres capas de supervisión. La primera es de carácter global, representado por instituciones y organizaciones de las que España es país miembro y que, por tanto, fijan estándares mínimos de actuación. La segunda sería regional, y en el caso concreto de España, se trataría de las instituciones y autoridades propias de la UE. Finalmente, a nivel local, el país (en este caso España) contará con sus propios mecanismos de supervisión. A su vez, estas tres capas se dividen en forma matricial por tres verticales de (i) banca y pagos, (ii) inversión y mercados de capitales y (iii) seguros. Esta clasificación en tres grandes grupos ha sido la base de la estructuración del análisis de los servicios *FinTech* en sus épocas disruptivas previamente abordadas.

### 3. Arquitecturas de supervisión

#### 3.1 Comités de coordinación a nivel europeo: el comité conjunto de autoridades de supervisión europeas

El Comité Conjunto de Autoridades de Supervisión Europeas (JCESA, por su siglas en inglés) surgió a raíz de la crisis de 2008, en la que se hizo evidente la necesidad de una

adecuada gobernanza y coordinación entre las autoridades de los tres verticales (banca, mercados financieros y seguros y planes de pensiones) con la finalidad de abordar las deficiencias identificadas en esta época, principalmente: (i) la falta de control sobre consecuencias secundarias de una crisis en un vertical (inversión) sobre el resto, (ii) la ausencia de reacción temprana y seguimiento adecuado del incremento de riesgo o amenaza, y (iii) la existencia de arbitrajes regulatorios en la zona europea o falta de igualdad de condiciones (European Union, 2016, pp. 7-11).

De este modo, se configuró el Sistema Europeo de Supervisión Financiera (ESFS, por sus siglas en inglés), que está compuesto de las tres autoridades europeas de supervisión (EBA, ESMA y EIOPA), la Junta Europea de Riesgo Sistémico (ESRB, por sus siglas en inglés), el JCESA y las autoridades competentes nacionales o europeas de cada Estado Miembro o región (European Union, 2016) (ver Figura 44).

El JCESA funciona como un nexo entre las autoridades competentes, permitiendo obtener posiciones de estandarización transnacional y transversal a banca, mercados y seguros y planes de pensiones (ver Figura 44). Entre sus principales tareas se encuentran las siguientes: (i) identificación y asesoramiento de riesgos derivados de los conglomerados financieros (implicaciones cross-sectoriales), (ii) establecimiento de estándares de supervisión en cuanto a informes regulatorios, informes contables y auditorías, (iii) detección de desarrollos intersectoriales a nivel microprudencial y macroprudencial que pueden impactar en la estabilidad financiera, (iv) protección al consumidor, innovación financiera y ciberseguridad, (v) prevención de blanqueo y financiación del terrorismo, (vi) intercambio de información y mejores prácticas entre autoridades y supervisores participantes, (vii) y otras actividades (European Banking Authority [EBA], 2022c, pp. 7-11).

Estas clasificaciones coinciden con los subsiguientes grupos de trabajo o subcomités con los que cuenta el JCESA, tal y como se puede observar en la Figura 45. Precisamente, el plan de trabajo de este comité, publicado el 29 de septiembre de 2021, cuenta con un claro enfoque hacia la innovación tecnológica, ya sea como un riesgo a monitorizar (*BigTech*) o como una oportunidad para explorar. En este segundo aspecto, el comité se enfoca en impulsar nuevas tecnologías como el uso de DLT, API, IA o *machine learning* como parte de la experimentación llevada a cabo por los facilitadores de innovación (Joint Committee of European Supervisory Authorities [JCESA], 2021, pp. 7-14). En concreto, el regulador europeo parece enfocar sus

esfuerzos hacia el nicho de *Green FinTech*, proponiendo *green sandboxes* o entornos de testeos supervisados (Financial Conduct Authority [FCA], 2021a, p.1). Estas iniciativas siguen el ejemplo de reguladores como el de Reino Unido, que durante 2021 y 2022 abrieron sus entornos controlados de pruebas a empresas que están desarrollando soluciones relacionadas con iniciativas de ESG. Dichos testeos, se centraron en soluciones de automatización de captura de datos, validación o auditoría e informes (Financial Conduct Authority [FCA]), 2021a, pp. 1-3).

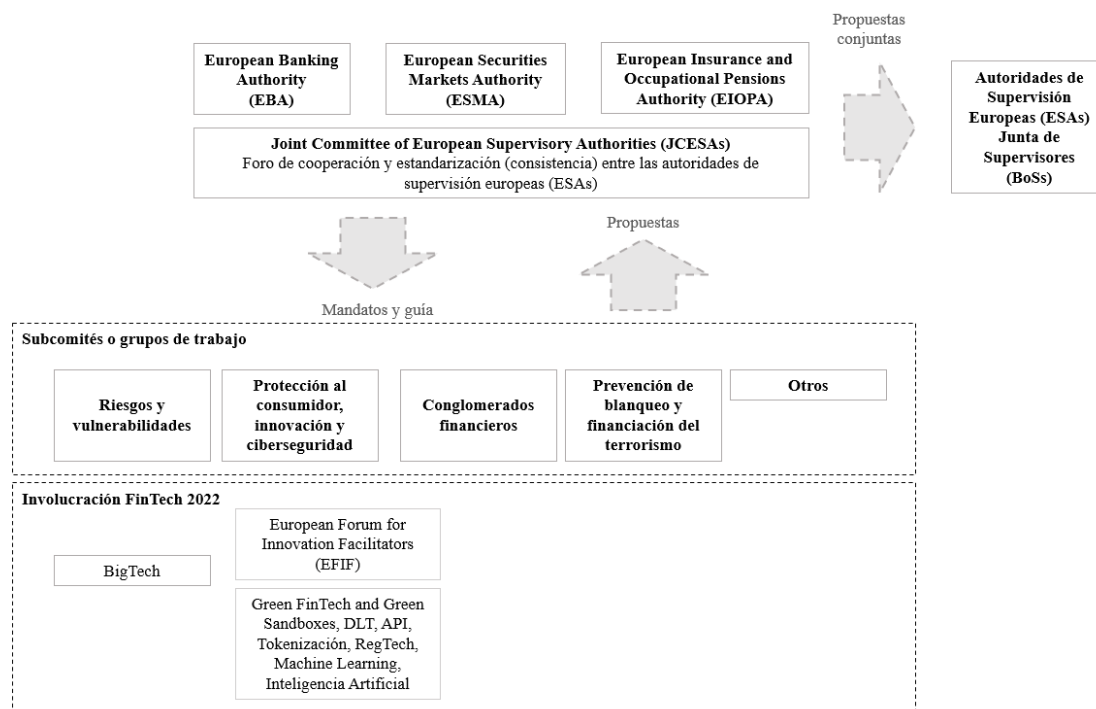


Figura 45. Estructura organizacional del JCESA y su involucración en asuntos de innovación de acuerdo con su plan de trabajo para 2022

Nota. Elaboración propia, adaptado de *Towards European Supervisory Convergence. the Joint Committee of the European Supervisory Authorities*, por European Union, 2016, European Union.

### 3.2. Mecanismo Único de Supervisión

Los antecedentes del MUS se remontan a la Comunicación de la Comisión COM (1999) 232, del 11 de mayo de 1999 (Commission of European Communities, 1999, pp. 1-28), en la que se resaltaba la necesidad de crear y mejorar el sistema de supervisión financiera, aumentando los esquemas de cooperación que hasta el momento se basaban principalmente en acuerdos bilaterales.

Este informe es respaldado por el llamado Informe Lamfalussy, que estableció el marco que lleva su propio nombre y que establece procedimientos de coordinación legislativa entre la Comisión, el Consejo y el Parlamento Europeo (The Committee of Wise Men, 2001, pp. 1-117). La propuesta de Lamfalussy (inicialmente enfocada en mercados de inversión) implica una estructura de cuatro niveles.

En el primer nivel, la CE propone regulaciones financieras, previa consulta con el Consejo y el Parlamento. Se trata de una estructura de codecisión. En el segundo nivel, la CE consulta a determinados comités regulatorios y recibe asesoramiento técnico de ciertos comités de supervisión. Los comités tienen capacidad de voto sobre las propuestas en este nivel, y la CE las adopta y las somete a un proceso de escalado (Hagenfeldt, 2009, pp. 3-4). Inicialmente, estos comités carecían de capacidad legal o recursos para llevar a cabo tareas de supervisión adecuadas, y se limitaban a elaborar informes técnicos en los que se basaban las directivas (Ortiz, 2018, p. 83).

El tercer nivel se centra en los detalles técnicos o de guías (asesoramientos técnicos de estandarización para los países). Sin embargo, no tienen capacidad sancionadora y se trata de mecanismos de *soft law* o recomendaciones (Hagenfeldt, 2009, pp. 3-4). Finalmente, el cuarto nivel se refiere a la monitorización y supervisión del proceso de transposición de la normativa europea a los regímenes locales de los Estados Miembros. Su incumplimiento es sancionable ante el Tribunal Justicia de la Unión Europea (TJUE) (Hagenfeldt, 2009, pp. 3-4).

Las debilidades de los comités consultivos de segundo nivel se abordan en la COM (2007) 727 del 20 de noviembre de 2007 y en la Directiva 2005/I/CE, en la que se reorganizan y se establecen comités especializados en el sector financiero (Ortiz, 2018, p. 83).

El MUS surgió como respuesta a la crisis de 2008 y al aumento de las actividades financieras fuera del perímetro supervisor de las autoridades nacionales o más allá de los límites de estas. La salida de flujos financieros fuera de los balances de las entidades financieras, aunque fue menos pronunciada que en el caso estadounidense, tuvo un alto impacto a nivel europeo. De este modo, el foco de supervisión experimentó una transición de enfoque: de las entidades financieras hacia los mercados y sus actividades (Kremers et al., 2003, pp. 2-7). Podría considerarse que se evidencia un giro de la regulación y

supervisión *entity based* (enfocada en sujetos obligados) hacia *activity based* (enfocada en actividades).

En 2012, el *Informe de los cuatro presidentes* (referente a los presidentes del Consejo Europeo, la Comisión Europea, Eurogrupo y el BCE) planteó formalmente la necesidad de avanzar hacia la unión económica y monetaria.

Un año más tarde, se publicó el Reglamento (UE) N.º 1024/2013 del Consejo, del 15 de octubre de 2013, que asignaba al BCE tareas específicas relacionadas con la supervisión prudencial de las entidades de crédito. Esto convirtió al BCE en el responsable del MUS, que se implementó efectivamente en noviembre de 2014. En el mismo año, se agregó la responsabilidad del MUS a través del Reglamento (UE) N.º 806/2014 del Parlamento Europeo y del Consejo, del 15 de julio de 2014, que establece normas y un procedimiento uniforme para la resolución de entidades de crédito y ciertas empresas de servicios de inversión en el contexto de un Mecanismo Único de Resolución y un Fondo Único de Resolución (European Central Bank [ECB], 2022b, pp. 1-5).

Respecto a la operativa del MUS, se basa en ciclos de mejora continua, generando retroalimentación a partir de las labores de supervisión realizadas con base en la normativa aplicable y proponiendo modificaciones basadas en los análisis realizados (ver Figura 46. Flujos operativos en el *Single Supervision Mechanism* (Mecanismo Único de Supervisión)). Se trata de un enfoque de arriba hacia abajo, es decir: políticas y normas, metodología y estándares, implementación, evaluación de calidad y propuestas de mejora.

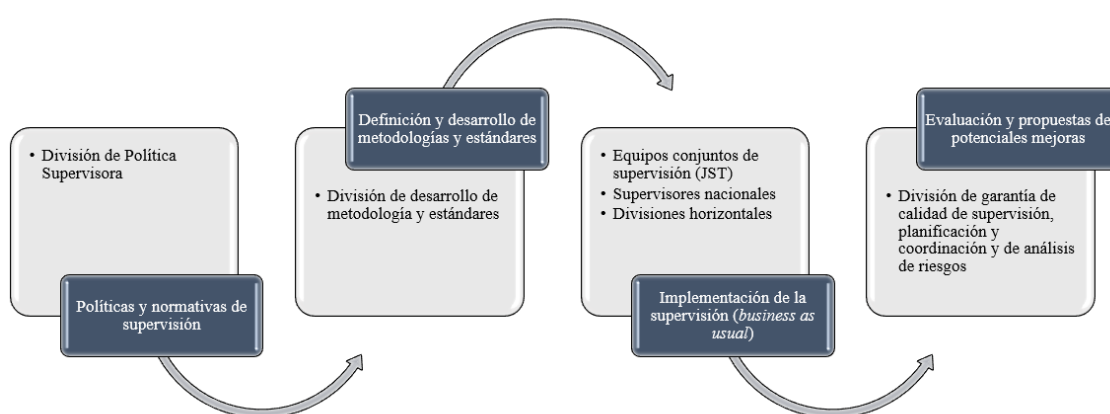


Figura 46. *Flujos operativos en el Single Supervision Mechanism (Mecanismo Único de Supervisión)*

*Nota.* Tomado de *Hitos*, por European Central Bank [ECB], 2022d, pp. 1-2 <https://www.bankingsupervision.europa.eu/about/thessm/html/index.en.html>

El MUS sigue los estándares mínimos establecidos por el Comité de Basilea, y se armoniza en la zona europea a través de un código normativo único que aplica a todas las entidades financieras que operan en la zona europea. De esta manera, los estándares globales en torno a la gestión y supervisión de riesgos financieros se ven implantados y ejecutados a través de este mecanismo operativo, junto con la regulación desarrollada en la zona (específicamente las normas CRD IV<sup>128</sup> y CRR<sup>129</sup>).

En cuanto a su contenido o mandato, los principales objetivos del MUS son: (i) garantizar la estabilidad financiera de la región mediante una mayor integración de las autoridades del sistema bancario, (ii) velar por la seguridad jurídica del sistema, asegurando su solidez, y (iii) garantizar una implementación adecuada de los criterios de supervisión, de manera uniforme y estandarizada en la UE (European Central Bank [ECB], 2022d, pp. 1-2). Bajo el amparo de esta herramienta, el BCE ha establecido los parámetros para determinar qué entidades del sistema financiero se consideran materiales o críticas y, por tanto, están sujetas a su supervisión directa<sup>130</sup>, y qué entidades están sometidas a supervisión indirecta. Lo anterior, con el fin de evitar nuevas crisis financieras como la desatada por Lehman Brothers.

Como se puede observar, se ha evolucionado de un enfoque descentralizado y de coordinación entre autoridades nacionales hacia una armonización de prácticas de supervisión y regulación sectorial que cada vez más parece llevar a la UE hacia un modelo de centralización. Esta tendencia centralizadora o de coordinación intensa se evidencia tanto por la aparición de supervisores regionales por verticales (ESMA, EIOPA y BCE) y transversales (Autoridad Europea de Protección de Datos, Autoridad Europea de Prevención de Blanqueo de Capitales), como en las herramientas regulatorias empleadas (aumento de los reglamentos de aplicación directa a los Estados Miembros como instrumento de política regulatoria en la región).

---

<sup>128</sup> Directiva 2013/36/UE del Parlamento Europeo y del Consejo, del 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (Texto pertinente a efectos del EEE).

<sup>129</sup> Reglamento (UE) N.º 575/2013 del Parlamento Europeo y del Consejo, del 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) N.º 648/2012 (Texto pertinente a efectos del EEE).

<sup>130</sup> Los criterios establecidos son: el tamaño (valor total de activos superior a 30 000 millones de euros), la importancia económica en un país o en la totalidad de la UE, las actividades transfronterizas (el valor total de activos es superior 5000 millones de euros y la ratio entre sus activos/pasivos transfronterizos y sus activos totales en más de otro Estado Miembro participante es superior al 20 %), o si la entidad ha requerido asistencia financiera pública.



Actualmente, esta estructura presenta dos inconvenientes en lo que respecta a la supervisión *FinTech*:

El primero se refiere al alto nivel de complejidad y falta de flexibilidad de este mecanismo, puesto que requiere la intervención de numerosas contrapartes y temáticas, restando dinamismo al proceso de supervisión.

El segundo inconveniente se relaciona con la delimitación tanto de aspectos temáticos como geográficos en el ámbito de la UE. Este factor provoca que elementos esenciales de ciertas actividades *FinTech* queden fuera del alcance del MUS. Por ejemplo, los modelos financieros con un enfoque significativo en la gestión de datos podrían quedar parcialmente regulados, lo que impide evaluar el impacto total de dichos modelos.

Otro caso se refiere a los gigantes tecnológicos, como se mencionó anteriormente, que solo se analizarían desde las perspectiva de las actividades financieras, careciendo de un supervisor con mandato suficiente como para poder evaluar el modelo de negocio integral, no solo como conglomerado financiero, sino también como conglomerado de negocios total (híbrido). Esto incluye las relaciones de dependencia entre las entidades del grupo y sus implicaciones en términos de accionariado, relaciones comerciales o miembros compartidos de consejos de administración.

En cuanto al aspecto geográfico, como se ha podido ver a lo largo de la investigación, los modelos *FinTech* 4.0 se caracterizan por actuar de forma agnóstica a cualquier jurisdicción, careciendo de estructuras organizativas concretas o asociadas a una única jurisdicción (especialmente en casos de DeFi con DAO como modelo de gobernanza). Ello hace que un mecanismo de supervisión regional pueda resultar inefectivo en este tipo de negocios que, además, operan con tecnologías incensurables.

En ese sentido, los criterios tradicionalmente considerados, como la jurisdicción sobre la materia, pueden volverse ineficaces, por lo que se requieren nuevos elementos más flexibles o indeterminados, como los indicios de materialidad en la región. Estos indicios podrían incluir la toma de decisiones centralizadas en un país o la distribución y comercialización masiva al público en una jurisdicción. No obstante, la aplicación de estas pautas también puede plantear riesgos, como la percepción de que los supervisores están aplicando un enfoque extraterritorial, algo que ya ocurre en la actualidad con normativas estadounidenses relacionadas con el crimen financiero, sanciones internacionales y evasión fiscal. Otro riesgo es el solapamiento con otros supervisores

debido a la falta de claridad respecto a la jurisdicción y la aplicación de criterios alternativos (menos definidos) para entrar a valorar el asunto en cuestión.

## II. LA TEORÍA DEL DESFASE SUPERVISOR

### 1. La problemática

Como se ha podido deducir a lo largo de este estudio, los modelos de producción normativa y supervisión no han sido capaces de adaptarse a estas nuevas realidades, especialmente en etapas caracterizadas como de disrupción o cambio de paradigma, cuyo origen son innovaciones *FinTech* (esto es, etapas *FinTech* 3.0-3.5 y 4.0).

Similar a los eventos que dieron lugar al informe Lamfalussy, la actualidad podría considerarse como paralela y, por tanto, da pie a cuestionar si las estructuras de supervisión actuales son adecuadas para las circunstancias vividas. La etapa actual en la que la vive la sociedad se ha clasificado bajo las siglas VUCA (Bennett y Lemoine, 2014, pp. 1-2). Este término corresponde a cuatro conceptos (*volatility*, *uncertainty*, *complexity* y *ambiguity*) que se describen a continuación, junto con las medidas o reacciones que exigen como factor mitigante.

El primer elemento se identifica como la volatilidad (*volatility*), entendida como los cambios drásticos, inestables, rápidos y frecuentes en el entorno, que a menudo son impredecibles o reducen la capacidad de reacción de las instituciones, incluyendo, a efectos de este trabajo, tanto instituciones privadas como públicas (reguladores y supervisores). La manera en la que se mitiga este riesgo es mediante un giro agresivo hacia la agilidad, hasta el límite que permita adquirir la capacidad de flexibilidad adecuada para hacer frente a estos cambios frecuentes (Bennett y Lemoine, 2014, p. 313).

El segundo elemento de los entornos actuales es la incertidumbre (*uncertainty*), entendida como la incapacidad del tomador de decisiones para obtener toda la información necesaria para tomar decisiones completas e informadas. En este entorno, el tomador de decisiones desconoce si comprende completamente un cambio, su origen y sus consecuencias o implicaciones. Esto lleva a la duda de si se enfrenta a un cambio material y si las medidas que se deciden son comprensivas o correctas (Millar et al., 2018, p. 7). Este riesgo es compensado mediante el replanteamiento de la gestión de la información para reducir la incertidumbre, incluyendo nuevas formas de colaboración y reciprocidad. Esto se alcanza adquiriendo nuevos puntos de acceso a datos y mejora de

conocimiento, por lo que se hace necesaria la búsqueda de nuevas fuentes de información que, a su vez, puedan ofrecer nuevas perspectivas (Bennett y Lemoine, 2014, p. 313). Ejemplos de posibles herramientas serían los *sandbox* regulatorios o la aplicación de tecnología para la obtención de una suerte de supervisión integrada (*SupTech*, abordado en capítulos anteriores).

El tercer componente es la complejidad (*complexity*), entendida como el aumento de causas, contrapartes y efectos para la toma de decisiones o medidas. La complejidad se eleva en casos en los que las causas o contrapartes nuevas aumentan, puesto que no existen antecedentes que puedan servir de referencia para el decisor (Lawrence, 2013, p. 5). Este tipo de situaciones pueden superarse a través de la reestructuración y simplificación con la finalidad de alcanzar una mejora en términos de eficacia y eficiencia de los procesos (Bennett y Lemoine, 2014, p. 313). También se deben incluir los cambios de actitud y la apertura o aumento de la interacción como elementos mitigantes.

El cuarto y último componente pertenece al concepto de ambigüedad (*ambiguity*), concebida como la falta de instrucciones claras y la dificultad para identificar las siete “W”: *who, what, when, how, where, why, how much*. Los marcos y reglas existentes no rigen las realidades y, por tanto, se produce una ruptura entre norma y realidad, no siendo claro si es aceptado o no. Es aquí cuando, tal y como defiende esta tesis, se dan eventos de lagunas normativas y, por ende, de supervisión. En estos casos, la experimentación permite obtener un mejor conocimiento y desarrollar nuevas estrategias, puesto que las normas y esquemas tradicionales se han vuelto ineficaces. Enfoques funcionales y pragmáticos, basados en principios, suelen ofrecer mejores respuestas en este tipo de circunstancias.

Estos cuatro elementos han impactado en los modelos de supervisión, lo que requiere un cambio en términos de agilidad, mejora en la gestión de la información, colaboración, reestructuración, flexibilidad, cambio de actitud, apertura, experimentación, enfoques funcionales y pragmatismo. Esta tesis defiende que la solución radica en una regulación que establezca principios como base para las nuevas formas de supervisión, incluyendo la autoregulación y la supervisión desde el diseño.

Esto se puede ilustrar gráficamente mediante un ejemplo de comparación de las líneas de tiempo de innovación, regulación y supervisión a lo largo de las etapas *FinTech* (ver figuras Figura 47, Figura 48 y Figura 49). Como se puede observar, inicialmente, cuando

se producía una innovación tecnológica en el mundo financiero, los reguladores y supervisores tenían la capacidad suficiente para reaccionar a tiempo mediante el estudio de la necesidad de producción normativa, implementación y supervisión. Sin embargo, a lo largo de las etapas *FinTech* 3.0 a 4.0, se ha observado un incremento exponencial de las innovaciones (recordar Figura 1. Evolución estimada de la capacidad tecnológica), al mismo tiempo que elementos como la globalización, la pertenencia a la UE y la cada vez más compleja estructura de supervisión nacional y supranacional han provocado una ruptura en la capacidad de los mecanismos de regulación y supervisión para poder responder a los cambios tecnológicos que están impactando en el universo financiero.

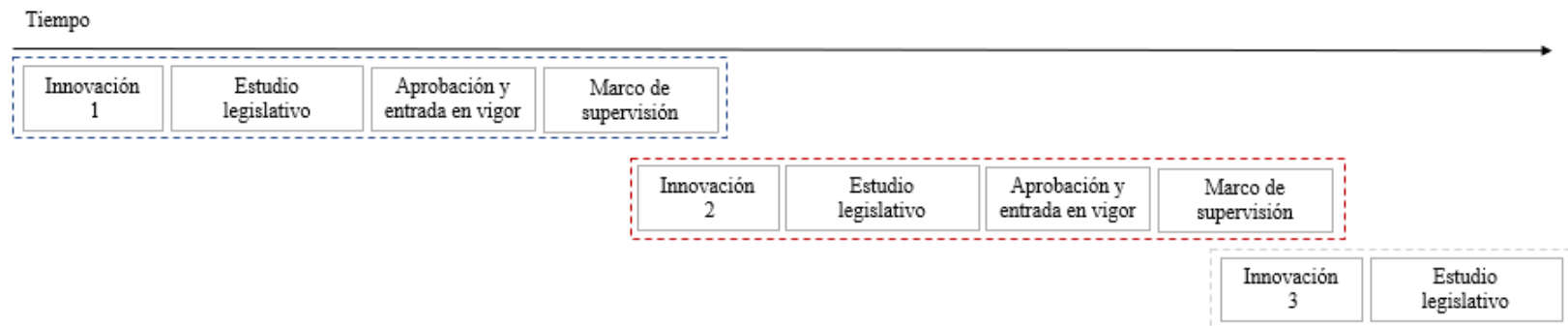


Figura 47. Ciclo de vida de innovación, regulación y supervisión en las etapas FinTech 1.0 y 2.0

Nota. Elaboración propia.

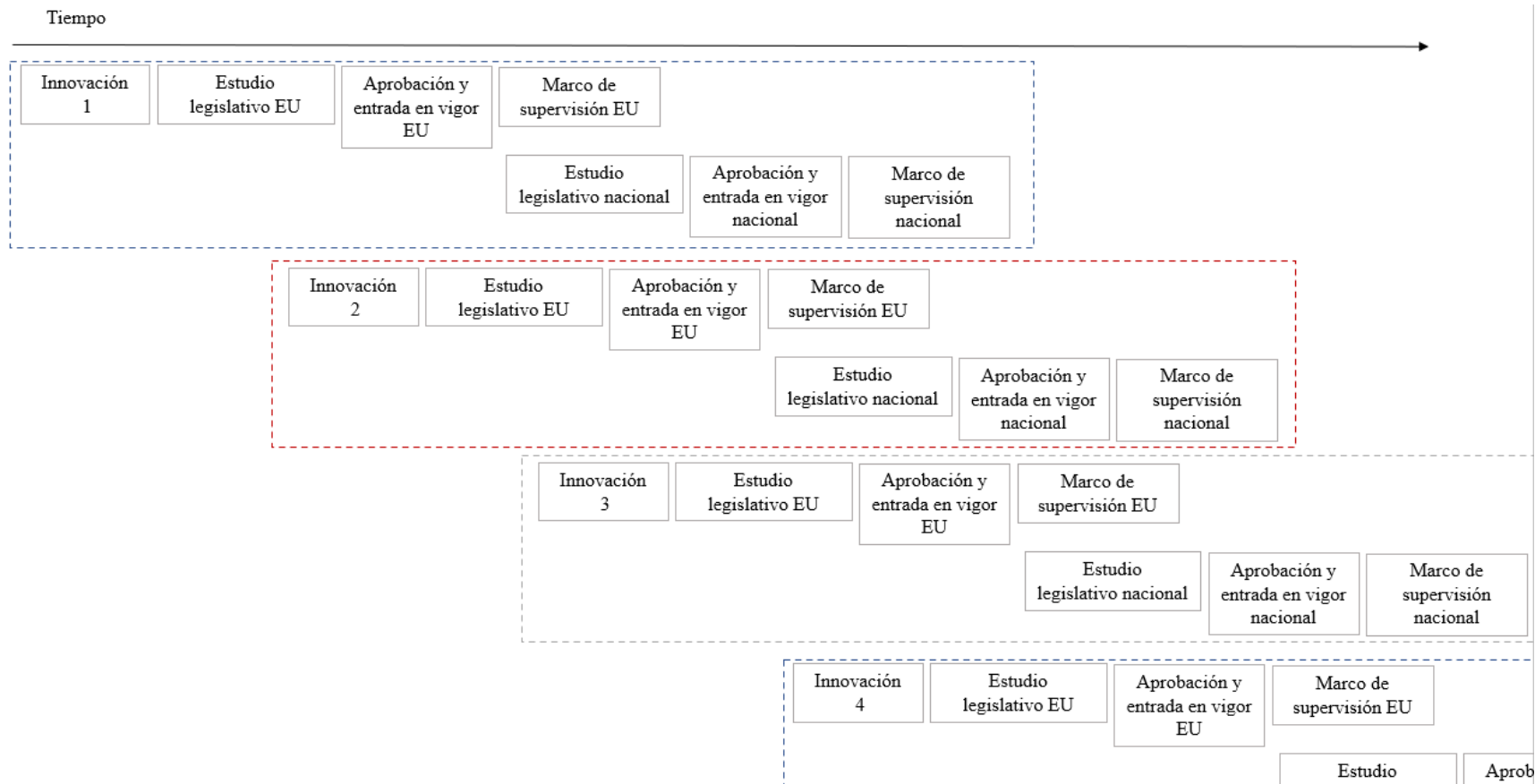


Figura 48. Ciclo de vida de innovación, regulación y supervisión en las etapas FinTech 3.0 y 3.5

Nota. Elaboración propia.

Tiempo

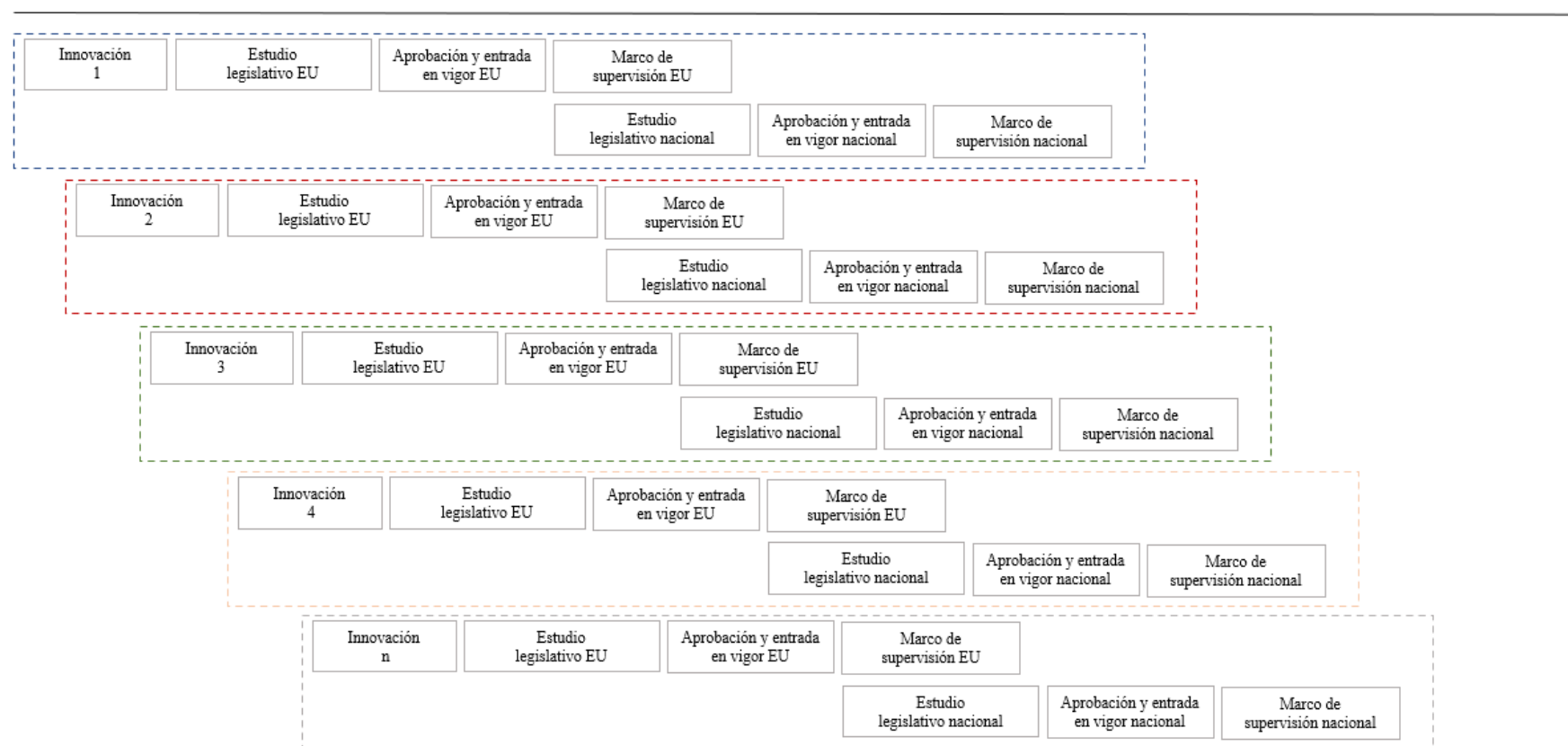


Figura 49. Ciclo de vida de innovación, regulación y supervisión en la etapa FinTech 4.0

Nota. Elaboración propia.

En efecto, en la actualidad existe un desfase entre los instrumentos públicos de regulación y supervisión *FinTech* y el progreso del sector privado. Ello se debe a varias causas de origen, que se pueden clasificar entre factores de demanda, que se refieren al sector privado en general, y factores de oferta, relacionados con la producción normativa y supervisión pública. A continuación, se desarrolla esta idea:

Desde el punto de la demanda (sector privado), ha habido un aumento exponencial de innovaciones con impacto en el sector en un corto periodo de tiempo, lo cual ha reducido la capacidad de gestión de estos por parte de las autoridades. Este componente puede identificarse con el término de volatilidad antes discutido.

Además, han aparecido nuevos agentes con distintos perfiles desde el punto de vista del tamaño (*start-up* y *BigTech*) y la actividad (origen tecnológico), creando modelos novedosos o híbridos que dificultan la determinación de los parámetros de supervisión. Estas particularidades pueden asociarse con los términos de incertidumbre y complejidad.

Finalmente, en la coyuntura de servicios de criptoactivos, se han producido situaciones de ambigüedad derivadas del hecho de que su adopción ha ido en aumento. Su esencia o naturaleza puede identificarse como de actividades de inversión o de pagos, pero la normativa no se aplica o solo se aplica parcialmente debido a que es incompatible con la realidad del negocio.

Desde el punto de vista de la oferta (sector público), el principal factor que puede delimitarse es la complejidad, entendida desde varios prismas:

- La coordinación del desarrollo normativo (por ejemplo, requiere normativa relacionada con la prevención de blanqueo, la protección de datos y la propia del sector financiero, creando requerimientos de acoplamiento entre distintos reguladores).
- La necesidad de producir normas y especificaciones técnicas de desarrollo de las normativas (por ejemplo, las directivas).
- La obligación de transposición a regímenes locales, aumentando los tiempos de aprobación administrativa.
- La exigencia de coordinar con otras autoridades a nivel internacional debido a la globalización.



La falta de conocimiento de estas innovaciones y su marcado componente tecnológico ha creado una brecha en términos de conocimientos técnicos y capacidad de asesoramiento por parte de las autoridades, derivado en incertidumbre de estas sobre cómo afrontar los retos que los nuevos agentes y operativas presentan. Tampoco es claro para las autoridades qué modelos de negocio emergentes se consolidarán y adoptarán frente a aquellos que no podrán sobrevivir o se descartarán.

Desde el punto de vista de la ambigüedad, los propios supervisores se enfrentan a la realidad de intentar encajar modelos híbridos o novedosos en los marcos regulatorios existentes, a pesar de que estos modelos se encuentran operando y tienen cada vez una mayor adopción por parte del público europeo. Prueba de ello son los avisos emitidos por autoridades europeas y Estados Miembros como España o Alemania sobre la publicidad de criptoactivos, a la espera de que finalmente se publiquen reglamentos que aborden esta problemática.

Además, la marcada volatilidad generada por la demanda (nuevos modelos, nuevas tecnologías, nuevos agentes) no ha sido acompañada de una mayor simplicidad, agilidad y pragmatismo por parte del sector público. Se observa una falta de reducción en los tiempos de producción normativa en comparación con la rapidez de los cambios en el mercado, como se verá en el caso del *travel rule* y su impacto en el conflicto bélico ruso-ucraniano.

Todos estos componentes llevan a la conclusión de que se ha identificado un desfase en la supervisión que requiere un replanteamiento del status quo actual, puesto que, de continuar así, se volvería ineficiente y se abrirían nuevos riesgos para los mercados y la sociedad, como se verá en el caso que se abordará a continuación.

## **2. Evidencia del desfase: el caso de la regulación del “*travel rule*”**

Un ejemplo claro del impacto de este denominado desfase supervisor se pone de manifiesto en la regulación relativa a la información que debe acompañar a las transacciones y su impacto en el conflicto bélico ruso-ucraniano.

Como se detalló anteriormente, desde junio de 2019, FATF ha realizado llamamientos a sus Estados Miembros, haciendo énfasis en la necesidad de que los proveedores de servicios cripto caigan bajo el paraguas de supervisión de las unidades de inteligencia financiera de los países y que se controlen las transacciones en sí, similar a como se viene

estableciendo en el mundo financiero tradicional desde hace años (Financial Action Task Force [FATF], 2021d, pp. 1-46).

De este modo, FATF exhortó a sus países miembros a que implementaran medidas regulatorias a este respecto. Sin embargo, en la segunda revisión realizada por el organismo dos años después, en el que hubo un total de 128 jurisdicciones participantes (Financial Action Task Force [FATF], 2021d, p. 10), se indicó que tan solo 23 jurisdicciones introdujeron el *travel rule*, siendo efectiva únicamente en 10 de ellas.

En el caso europeo, el Reglamento MiCA y el Reglamento del “*travel rule*” que fueron aprobados el 9 de junio de 2023, no cubren casos en los que no exista un mediador o tercero de confianza, como puedan ser las billeteras cripto no atendidas o los operadores descentralizados. Esta actividad, cuyo riesgo se identificó en 2019 y que se ha mantenido sin una solución viable regulatoriamente durante tres años, resultó ser de imperativa necesidad en febrero de 2022 a raíz del conflicto ruso.

Con el inicio de los ataques sobre Ucrania, Estados Unidos, la UE y Reino Unido, entre otros, comenzaron a publicar sanciones financieras internacionales desde el 21 de febrero de 2022, cuyo objetivo era el bloqueo de activos y contrapartes ligadas al régimen ruso (White House, 2022, pp. 1-4). Entre estas medidas, se encontraba la exigencia de que entidades rusas que operaban en el sistema financiero de forma global a través de SWIFT fueran expulsadas del sistema y, por tanto, de las infraestructuras de pago mundiales (SWIFT, 2022a, p.1).

Las listas de contrapartes sancionadas, una vez actualizadas, deben verificarse en todas las operaciones llevadas a cabo por las instituciones financieras, aplicando la normativa de la información que debe acompañar a las operaciones y la debida diligencia que se debe aplicar a todas las transacciones, también conocida como *know your transaction* (KYT) o “conoce tu transacción”.

Sin embargo, estas medidas aún no se aplican a las operaciones de criptoactivos, lo que generó un vacío regulatorio que fue aprovechado como medio de supervivencia para los flujos financieros rusos, evitando así los mandatos de sanciones financieras internacionales. Una prueba de ello fue el aumento de volúmenes y los cambios de rublos a criptoactivos que se experimentaron tras la publicación de las órdenes de embargo (Willson, 2022, p.1).

Efectivamente, existen evidencias de que el riesgo identificado por FATF desde hace varios años se ha materializado en el conflicto, sin que haya sido ningún tipo de mecanismo *fast track* que permitiese implementar el reglamento de manera oportuna. Además, el retraso en este tipo de implementaciones ha desincentivado al sector privado a invertir en la búsqueda de posibles herramientas y soluciones que puedan implantarse de forma global, eficiente y escalable (Financial Action Task Force [FATF], 2021d, pp. 1-46).

Finalmente, es importante destacar que incluso tras la implementación de este reglamento, se ha dejado sin control a los protocolos descentralizados, lo que fomentará el aumento de movimientos evasivos hacia este tipo de servicios.

Otro aspecto que se debe tener en cuenta es que gran parte de estos flujos son internacionales, lo que puede dar lugar a transacciones en las que una parte esté sujeta a las obligaciones en una jurisdicción donde se haya implementado esta medida, mientras que la otra parte se encuentre en un país que aún no haya implementado este requisito, lo que genera incertidumbre sobre cómo operar y posibles lagunas regulatorias.

### **III. SANDBOX REGULATORIO. CONTROVERSIAS DE POLÍTICA JURÍDICA**

Los *sandboxes* regulatorios o entornos controlados de prueba permiten que diversos proyectos de innovación *FinTech* que carecen de encaje regulatorio local puedan ponerse en marcha, de una forma controlada, para poder ser testados y, a su vez, para que el supervisor pueda asesorar los riesgos y controles requeridos, e incluso la potencial necesidad de desarrollo o adaptación de normativa local. En ese sentido, las partes (promotor y supervisor) acuerdan previo a su lanzamiento un marco de control específico para la iniciativa que, incluso, puede llegar a permitir exenciones de ciertos requisitos regulatorios. Estos pilotos se encuentran acotados en varios aspectos, como el público objetivo, los volúmenes, el ámbito temporal e incluso la materia (innovaciones financieras con potencial impacto en el mercado y que carecen de marcos regulatorios claros) (Suárez, 2021, pp. 183-229).

Por tanto, los entornos controlados de pruebas operan como una vía de escape a los entornos regulados en los que deberían de operar, pero carecen del encaje adecuado para dar cabida a estas innovaciones financieras (Zunzunegui, 2020, pp. 1-21). De esa manera, la proliferación de *sandbox* en la UE ha ido en aumento debido la fuerza que ha cobrado la innovación e incertidumbre sobre cómo afrontarla.

La cuestión de fondo respecto a los entornos controlados de pruebas es el motivo por el que se desarrollan. Se puede hablar de una búsqueda de entendimiento por las partes como primer paso: el supervisor busca comprender la nueva tecnología y su aplicación, mientras que el promotor busca comprender las expectativas regulatorias y la viabilidad del producto o servicio. Como segundo paso, de mayor profundidad, se identifican con objetivos como aumentar la competitividad, brindar un mejor servicio a los agentes, mejorar la gestión de riesgos y promover la inclusión financiera (Suárez, 2021, pp. 183-229).

Sin embargo, en línea con las reflexiones que se llevarán a cabo más adelante, se considera que la verdadera finalidad del desarrollo de estos no es otra que la de identificar lagunas normativas, evaluar y reinterpretar los marcos normativos para poder avanzar con estas novedades otorgando ciertos niveles de seguridad jurídica a las partes y al mercado. Es decir, se interpretan los entornos de pruebas controlados y supervisados como áreas en las que el supervisor opera de forma similar a un juez al aplicar la analogía para poder resolver situaciones materiales que requieren una respuesta.

En consecuencia, los entornos controlados de pruebas no pueden ser considerados como una estrategia que resuelva toda la incertidumbre de la falta de encaje normativo de actividades *FinTech*, sino que son herramientas tácticas de identificación y solución a corto plazo para evitar casos graves de inseguridad jurídica. Desde el punto de vista del supervisor, estas herramientas les permitirán detectar barreras regulatorias que desembocarán en cambios de normativas existentes o el desarrollo de nuevas regulaciones. También permitirán mitigar los riesgos de incumplimiento por parte de los promotores de los proyectos, así como mejorar los niveles de entendimiento mutuo (modelo de negocio, potencial, riesgos y entornos de control requeridos) (Suárez, 2021, pp. 183-229).

Por su parte, la UE ha comenzado a regular *sandbox* a nivel regional para ciertos casos de alto potencial en los que el sistema regulatorio actual supone un corsé al que la tecnología claramente no puede adaptarse. Este es el caso del régimen piloto de tecnología de registros distribuidos<sup>131</sup> para infraestructuras de mercados. En ese sentido, se ha regulado a través de un reglamento de aplicación directa a todos los Estados Miembros

---

<sup>131</sup> Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) n° 600/2014 y (UE) n° 909/2014 y la Directiva 2014/65/UE.

un contexto que permite experimentar con *Blockchain* aplicando excepciones a la normativa actual, especialmente MiFID II. Este reglamento será objeto de análisis crítico más adelante.

Si bien esta herramienta presenta un gran paso adelante hacia una mayor flexibilidad, no deja de tener importantes limitaciones, como la falta de conocimiento, tiempo y recursos. Principalmente, los entornos controlados de pruebas requieren recursos (humanos, técnicos y tiempo) y tan solo un número limitado de participantes puede acceder a ellos, lo que implica que no son soluciones escalables. Por esta razón, la posición que se defiende en esta tesis es la de valorarlos como herramientas tácticas que forman parte del conjunto de medidas que colaboran en el desarrollo de la innovación a nivel regional.



## **CAPÍTULO VI. REGULAR *FINTECH*: ESTADO ACTUAL Y PROPUESTA A FUTURO**

### **I. PLANTEAMIENTO**

#### **1. Modelos de regulación *FinTech* y potenciales mejoras**

El presente capítulo tiene como objetivo identificar las tipologías de regulación bancaria en general y describir los flujos y procesos requeridos para el desarrollo de regulación. Posteriormente, se debate si es necesario o no regular *FinTech*, proponiendo potenciales modelos de regulación con especial foco en la propuesta de una regulación marco para modelos *FinTech* 4.0 debido a su radical diferencia. También se proponen cambios en la cuestión de los regímenes de licencias aplicadas a estos nuevos actores, así como un avance sobre potenciales modelos de supervisión. Como se expuso en la primera parte de este trabajo, exigen nuevos actores, por lo que se lleva a cabo una reflexión sobre cuál sería el ámbito subjetivo de aplicación de potenciales normas *FinTech*.

Más adelante, se explora por qué es necesario un nuevo planteamiento regulatorio, llegando a la identificación de la problemática de fondo. Es decir, la insuficiencia de una solución satisfactoria mediante la aplicación de la analogía y la identificación de la figura de la laguna normativa como base del problema al que se enfrenta el supervisor cuando se analiza el fenómeno *FinTech* como disrupción y cambio de paradigma.

Las conclusiones y evaluaciones realizadas en este capítulo se reflejan en los análisis críticos de las propuestas normativas europeas que se llevan a cabo en el capítulo siguiente.

#### **2. Tipologías de regulación bancaria en general**

La regulación bancaria, entendida como toda figura de control regulatorio ejercida por instituciones públicas, puede categorizarse, según Dragomir (2010, pp. 53-59), en función del objetivo que busca o los efectos en los agentes del mercado que regula. La taxonomía de producción regulatoria en función de su objetivo puede agruparse en tres grandes conceptos de riesgo de conducta, regulación prudencial y regulación de reacción o protección (Dragomir, 2010, pp. 53-59).

La primera de ellas se enfoca en la transparencia, gestión de conflictos de interés y objetividad de las contrapartes, siendo, por lo general, una regulación prolífica y detallada. Un ejemplo de ello es MiFID II. Por esta razón, la mayor parte del enfoque de este tipo de normativas es *ex ante* o de prevención de un riesgo (de mala conducta o de prácticas inapropiadas por parte de los agentes supervisados). La regulación prudencial, al igual que la de riesgo de conducta, es prolífica y detallada en la UE, con mayor peso en la prevención. Se centra en la estabilidad financiera, la solvencia del sistema bancario y la protección a consumidores (principalmente de los depósitos) (Dragomir, 2010, pp). Finalmente, la regulación de reacción o protección se enfoca en los escenarios de reorganización, rescate o resolución de las entidades del mercado, por lo que se puede considerar que su peso está en situaciones *ex post* (Dragomir, 2010, pp. 53-59).

Respecto a la regulación basada en los efectos, Dragomir distingue entre regulación bancaria prescriptiva y la regulación basada en acuerdos o incentivos.

El primer tipo de regulación, propia de entornos europeos, se basa en normativas o reglas que establecen las reglas del juego entre los participantes, proveyendo al sistema de seguridad jurídica y claridad en lo que las partes esperan las unas de las otras. Sin embargo, este tipo de normativa es poco flexible, por lo que puede caer en excesivo detalle, desactualización rápida y dar a entender que aquello que no esté contemplado en la regulación no tiene por qué controlarse o seguirse. Según Dragomir (2010), “rules can never encompass all facets and cannot catch all dynamic aspects of the market” (pp. 53-59). En consecuencia, este tipo de soluciones normativas no pueden considerarse como adecuadas en situaciones de incrementos repentinos de nuevos negocios, contrapartes e innovaciones como el que se está viviendo en la actualidad.

El segundo modelo de regulación, propia de los entornos anglosajones, se basa en soluciones de colaboración público-privada. Este tipo de formatos se fundamenta en principios y objetivos, dejando libertad al sector privado sobre cómo cumplir (Dragomir, 2010, pp. 53-59). Este patrón regulatorio se complementa en países como Reino Unido con aclaraciones prácticas de las expectativas supervisoras que tienen un carácter más dinámico, pueden actualizarse con mayor facilidad y adaptarse a cambios en las innovaciones. Un ejemplo de ello es el *UK FCA Handbook*, disponible electrónicamente para el público por parte del supervisor inglés (Financial Conduct Authority [FCA], 2022b). De esa manera, se promueve un enfoque basado en riesgos y más dinámico que



permite reaccionar en función de los cambios en los perfiles de riesgo inherente de la actividad y los agentes financieros operativos.

### **3. Flujos de producción normativa**

Los flujos de producción normativa, según su origen, podrían clasificarse como ascendentes o descendentes. Los primeros (ascendentes) son una reacción ante situaciones en los mercados locales. En el caso europeo, se pueden identificar escenarios en los que se hayan detectado desarrollos normativos locales dispares entre jurisdicciones o situaciones en las que algunos Estados Miembros hayan regulado mientras que otros no lo hayan hecho. Ante el riesgo de arbitrajes en la región, las autoridades europeas reaccionan mediante la elaboración de normas con el fin de estandarizar y restablecer el equilibrio en el mercado.

En el caso de la creación de normas descendente, esta se origina por iniciativas globales de coordinación global entre países (G20), instituciones (Comité de Basilea, IOSCO) u organismos de estandarización de determinadas temáticas (FATF). A raíz de sus estudios, recomendaciones y evaluaciones de impacto, la UE puede tomar la iniciativa de proponer estándares mínimos en la región con el fin de coordinar y mitigar los riesgos identificados globalmente.

Los instrumentos empleados por la UE pueden ser las directivas o los reglamentos. Las directivas requieren un desarrollo local por parte de los Estados Miembros y, por tanto, tienen el riesgo de extenderse en el tiempo. Además, este tipo de instrumento suele concluir en interpretaciones diferentes por parte de cada jurisdicción local, e incluso puede regular aspectos de forma no coordinada, añadiendo barreras o requerimientos (el denominado *gold plating*).

El segundo instrumento normativo por parte de la UE son los reglamentos. Esta solución tiene aplicación directa en los Estados Miembros y no requiere ningún tipo de desarrollo normativo local. Por ello, en el ámbito *FinTech*, se ha podido observar un incremento en los últimos años de reglamentos frente a directivas. Dado que las operaciones *FinTech* son, por naturaleza, transnacionales, es imprescindible establecer criterios homogéneos en la región para evitar fragmentaciones o interpretaciones dispares que puedan llevar a arbitrajes regulatorios en la UE.

En ambos casos, existen mecanismos de desarrollo que ofrecen aclaraciones y mayor detalle, incluyendo aspectos técnicos, formatos e interpretaciones entre las directivas y reglamentos.

#### **4. Procesos operacionales de desarrollos regulatorios**

Los procesos de desarrollo normativo podrían asemejarse a las metodologías de mejora continua de Toyota, en la que se pueden identificar cuatro grandes pasos conocidos como PDCA: planear (*plan*), hacer (*do*), comprobar (*check*) y actuar (*act*) (Liker, 2006, pp. 366-388) (ver Figura 50).

Por lo general, la fase de planificación da su pistoletazo de salida una vez que la cuestión ha alcanzado una masa crítica o una relevancia de impacto para considerarse como una prioridad de desarrollo de políticas públicas.

En el caso concreto de los desarrollos *FinTech 3.0* a *4.0*, la discusión no se centra tanto en su impacto actual (especialmente en *FinTech 4.0*), sino en la velocidad de su crecimiento y su potencial futuro. El crecimiento de estas innovaciones y su extensión podría dibujarse en una figura similar a un palo de hockey<sup>132</sup>, mientras que la gráfica equivalente a un proceso regulatorio sería más bien una progresión lineal ascendente. Esto provoca que la brecha entre innovación y regulación sea cada vez mayor. En esta primera etapa, también deben apreciarse elementos como qué autoridad cuenta con el mandato en la materia, la tipología de la normativa que se estaría desarrollando, las condiciones de mercado y las dinámicas entre sus agentes o las capacidades internas del regulador (The World Bank Group, 2020, p. 10).

Respecto a la fijación de prioridades de desarrollos normativos, cabe señalar que a menudo las producciones normativas se ven afectadas por las agendas de los partidos políticos en el poder, el nivel de conocimiento en la materia y la importancia que el público le ha dado. Una vez que se ha identificado la prelación de las temáticas a abordar, se realiza una evaluación de las condiciones y la viabilidad, así como una identificación de los objetivos y los indicadores de éxito de las medidas a implementar, que deberán ser evaluados en etapas posteriores.

La fase de asesoramiento incluye el mapeo del entorno regulatorio, el detalle de los riesgos y oportunidades, el crecimiento del mercado y sus agentes, así como la evolución

---

<sup>132</sup> Ver Figura 1. Evolución estimada de la capacidad tecnológica.

o madurez del tema objeto de análisis (en este caso, *FinTech*). En el caso *FinTech*, esta fase se ha visto afectada debido al alto componente tecnológico y la necesidad de conocimientos técnicos al respecto, los cuales actualmente están concentrados en el sector privado. Por lo tanto, ciertas jurisdicciones han optado por aumentar su interacción con expertos del sector privado y la academia (The City of London, 2021, p. 4).

Una vez que el asesoramiento se ha completado, se plantea la estrategia normativa a llevar a cabo, dando inicio a lo que equivalente a la segunda etapa en la metodología Toyota (*do*). Esta puede llevar a un amplio rango de respuestas, tales como (i) esperar y ver qué sucede (en el caso de que el análisis haya concluido que la innovación aún no es relevante); (ii) examinar y aprender caso por caso (puede aplicarse cuando se trata de una innovación con gran potencial, pero que aún no cuenta con suficiente aceptación o agentes que la ofrezcan); (iii) facilitadores de innovación (se refiere a casos de hubs de innovación o *sandboxes* regulatorios en los que el supervisor interactúa con el promotor para comprender mejor los nuevos modelos de negocio); (iv) reinterpretación de la regulación vigente o cambios normativos en estructuras existentes; y (v) desarrollo de piezas normativas *ad hoc* (The World Bank Group, 2020, p. 10).

El tercer estadio de comprobación (*check*) comprende el análisis y la evaluación de las medidas implantadas y su adecuación a la situación. En esta etapa, se suele lanzar consultas a los supervisores para conocer su problemática en la puesta en práctica de la regulación. Además, se obtiene información sobre métricas de éxito que se hayan considerado en la fase de planificación por parte de la administración pública, con el fin de identificar si la regulación ha tenido el efecto esperado (por ejemplo, el aumento de los agentes en el mercado, la reducción de la inseguridad jurídica o la mejora de la protección a consumidores).

Con base en los resultados obtenidos en la tercera fase, se abriría el cuarto paso, esto es, actuar (*act*). En este punto, las autoridades deben considerar el mantenimiento del contexto regulatorio actual, la necesidad de acometer ajustes o, incluso, la iniciativa de un entorno normativo nuevo (The World Bank Group, 2020, p. 10). De esta forma, el círculo de mejora comenzaría de nuevo, al plantearse cambios normativos sobre estructuras existentes.

En el caso europeo, como se expuso anteriormente, es importante destacar que este proceso operativo se desarrolla en al menos dos niveles (el europeo y el nacional), e

incluso podría haber un tercer nivel (global-europeo-nacional), lo que añade una mayor complejidad.

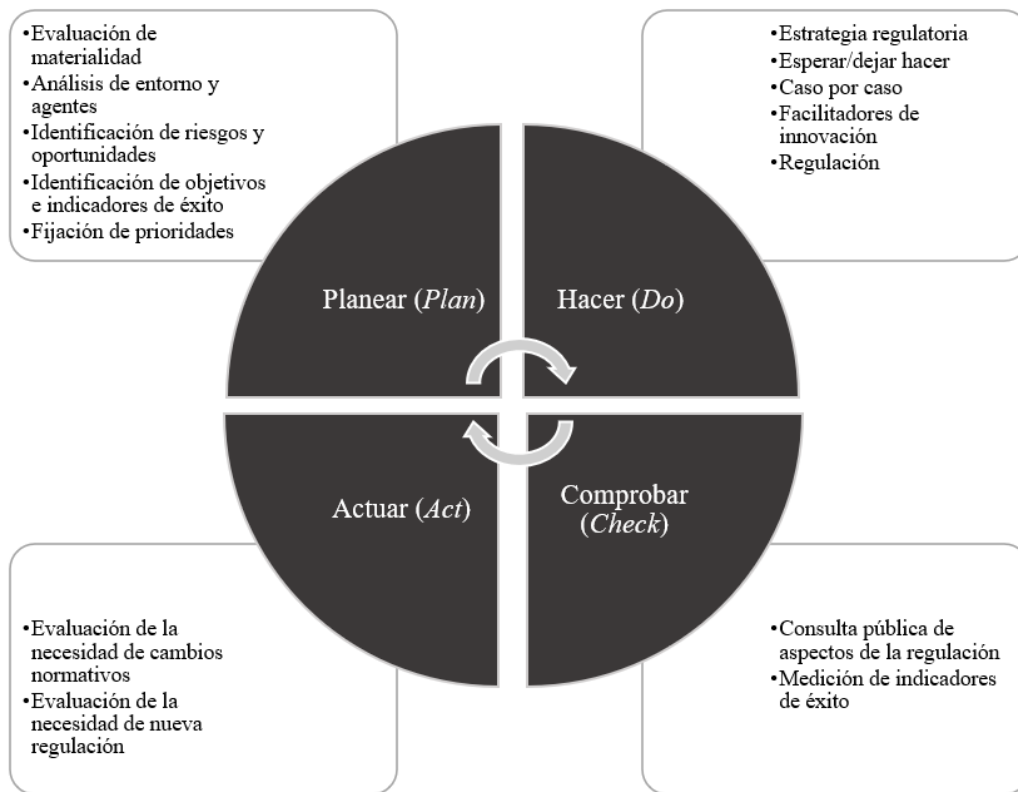


Figura 50. Metodología PDCA aplicada a los procesos de producción normativa FinTech

Nota. Elaboración propia.

## II. OPCIONES DE POLÍTICA JURÍDICA. PRINCIPIOS RECTORES

Ante la proliferación de innovaciones financieras y nuevos agentes, cabe plantearse la pregunta de si todo *FinTech* debe estar regulado y si este tipo de entidades deben estar sujetas a regímenes de registro o licencia. En los casos de reguladores exhaustivos, la tentación de extender regímenes existentes a los nuevos modelos puede ser alta; sin embargo, este tipo de enfoques puede adolecer de ciertas desventajas que se detallan a continuación.

Un desarrollo normativo exhaustivo puede desembocar en ineficiencias de las estructuras normativas y de supervisión. Esto se debe a que un excesivo efecto fiscalizador puede derivar en esfuerzos normativos desproporcionados, que frenarían el incentivo a la innovación en la jurisdicción correspondiente. Por tanto, conllevaría la huida del talento a regiones más amigables y resultaría en un inadecuado uso de los

recursos en los casos en los que la innovación aún se encuentre en una fase prematura (Enria, 2018, pp. 2-3). Además, una posible regulación precoz de la tecnología podría entrañar un mal entendimiento de esta, aplicando una extensión de la normativa vigente a los nuevos modelos (analogía), aunque esta no se adecúe a estas nuevas realidades, o incluso prohibiendo su funcionamiento en la jurisdicción.

Igualmente, los procesos normativos, que de por sí complejos y largos, podrían hacer que, en el momento de la publicación de la normativa, esta ya esté desactualizada (como ocurre en la actualidad en las políticas regulatorias europeas<sup>133</sup>). Verdaderamente, la opción de regulación exhaustiva no parece ser el desenlace óptimo para las innovaciones disruptivas en el sector financiero. Tan solo podría plantearse parcialmente, para determinados aspectos de alto riesgo, como pudiera ser de crimen financiero, protección de datos, transparencia o riesgo de conducta.

Por el contrario, una estrategia de esperar y no regular puede derivar en serios riesgos de estabilidad financiera y de protección a consumidores, puesto que los nuevos modelos pueden adoptarse y crecer con una rapidez mayor a la vista hasta ahora (especialmente, durante la COVID-19 y el conflicto ruso-ucraniano se evidenció la capacidad de escalado y crecimiento de estos negocios en cuestión de meses).

Una posición *laissez faire* podría avocar a un aumento del riesgo sistémico fuera de los entornos regulados y, por tanto, de supervisión, no pudiendo asesorar las relaciones e interdependencias entre los actores regulados y los no regulados, tal y como sucedió en la crisis de 2008 (Enria, 2018, pp. 2-3). Por consiguiente, los desarrollos normativos en aspectos *FinTech* deberían basarse en modelos similares al anglosajón, esto es: normativas basadas en principios que puedan complementarse con instrumentos de política normativa secundarios y más ágiles, como guías o manuales emitidos por las autoridades supervisoras. Este enfoque en principios podría ser lo suficientemente genérico como para no requerir actualizaciones constantes y abarcar nuevas innovaciones. Los desarrollos de nivel inferior (más ágiles) establecerían de manera dinámica las expectativas supervisoras. De esta manera, se lograría una mayor adaptabilidad, un equilibrio adecuado entre el costo de los recursos y la efectividad, y se

---

<sup>133</sup> Esta declaración se sustenta mediante el análisis crítico de ciertas regulaciones *FinTech* en el Capítulo CHAPTER VII. CRITICAL ASSESSMENT OF SPECIFIC REGULATORY INITIATIVES.

reduciría la necesidad de cambios normativos constantes, puesto que estos se abordarían en los instrumentos secundarios (Amstad, 2019, pp. 1-17).

Esta tesis defiende que este tipo de propuestas deben seguir ciertos principios que se delimitan a continuación.

En primer lugar, se encuentra el principio de misma actividad, mismos riesgos, misma regulación: con la finalidad de evitar arbitrajes o problemáticas de competencia, aquellas actividades cuya sustancia sea equivalente a otras reguladas deberán considerarse en el ámbito de aplicación normativo. Ello no supone que la normativa existente no esté exenta de revisión debido a que haya podido quedarse parcialmente desactualizada o porque haya perdido su eficacia debido a los cambios ocurridos en los mercados financieros con la irrupción de nuevas tecnologías.

En concreto, esta máxima se ha mencionado reiteradamente en distintas organizaciones y autoridades con respecto a cómo gestionar el fenómeno *FinTech*, como base para asimilarse a regulaciones existentes (Lautenschläger, 2017, pp. 1-3; Hoyler, 2022, pp. 1-2; European Banking Federation [EBF], 2022b, pp. 1-24; Wuermeling, 2022, pp. 1-7). Por este motivo, en la siguiente sección se realiza un análisis crítico. A pesar de que es un principio ampliamente discutido, no ha sido adecuadamente reflejado en las nuevas iniciativas regulatorias, a diferencia de lo que ocurre con otros principios como el de proporcionalidad.

Este axioma está íntimamente relacionado con el concepto de igualdad de condiciones o *level playing field*, por el que se exige que todos los participantes en similares circunstancias operen bajo las mismas reglas.

En segundo lugar, se halla el principio de proporcionalidad (Amstad, 2019, p. 6) y enfoque basado en riesgos. Si bien es cierto que algunos modelos *FinTech* suponen ejercer el mismo tipo de actividades reguladas, con riesgos similares, frecuentemente detrás de estos modelos se encuentran empresas de menor tamaño o de origen exógeno al mundo financiero, por lo que es necesaria la aplicación de criterios de proporcionalidad y enfoque basado en riesgos. Es precisamente este aspecto el que puede resultar trascendental tanto para los *incumbents* como para los nuevos participantes; sin embargo, en general, no suele aplicarse en la práctica debido a la perspectiva conservadora de los supervisores en este ámbito. De este modo se evaluaría en nivel de riesgo que la actividad presenta para así indicar los requisitos regulatorios que le aplican en consecuencia. Las

contrapartes y actividades de mayor riesgo estarán sujetas a exigencias más intensivas en términos de recursos, mientras que las de menor riesgo disfrutarían de una condiciones más flexibles.

En tercer lugar, está el principio de delegación. Este principio se refiere al hecho de que, en ocasiones, las *FinTech* no serán sujetos obligados directos, sino sujetos obligados indirectos (proveedores de entidades reguladas y sujetas al perímetro supervisor). De este modo, la capacidad de supervisión y regulación de autoridades se delega en los sujetos obligados o regulados, quienes establecerán marcos normativos entre contrapartes privadas por vía contractual y perímetros de supervisión mediante el ejercicio de auditorías o diligencias debidas de sus órganos de control interno (auditoría, riesgos y *compliance*, principalmente). No se trata de una idea nueva, sino que ya se ha venido aplicando este ángulo al desarrollar normativas que aluden a las funciones de auditoría interna, riesgos o cumplimiento normativo (la imposición de estas en las entidades reguladas no viene sino a suponer una privatización de la labor de control de los entes públicos).

En cuarto lugar, se encuentra el principio de neutralidad tecnológica (Enria, 2018, pp. 6-7), por el cual el regulador debe centrarse en la actividad, evitando indicaciones referentes al uso de tecnologías específicas. A modo de ejemplo, la actividad puede ser aparentemente igual de cara al cliente final, pero la tecnología empleada puede abrir la puerta o alterar los riesgos reales que subyacen a la operativa. Las entidades deben tener en cuenta estos elementos como parte de su evaluación de riesgos y gestión de controles para mitigarlos (es decir, la tecnología empleada caería dentro del entorno de la gestión privada de riesgos). Un ejemplo de ello ha sido el enfoque del Comité de Basilea respecto a la exposición de riesgos cripto en la banca (Basel Committee on Banking Supervision, 2022, pp. 2-3). Si bien el planteamiento inicial exigía una penalización en los ratios de capital de los bancos por el uso de infraestructuras DLT, finalmente se ha optado por un enfoque más flexible<sup>134</sup>. De haber avanzado la propuesta inicial, se habría atentado claramente contra la neutralidad tecnológica.

---

<sup>134</sup> Finalmente, se contempla que “En la segunda consulta, el complemento para el riesgo de infraestructura se propuso como un complemento fijo para el conjunto de activos ponderados de riesgo o RWA al 2,5 % del valor de exposición para todos los criptoactivos del Grupo 1. El Comité acordó reemplazar esto con un enfoque más flexible que permite a las autoridades iniciar y aumentar un complemento basado en cualquier observado debilidades en la infraestructura que subyace a criptoactivos específicos. Este enfoque debería incentivar bancos para abordar activamente los riesgos de infraestructura para evitar la imposición de un complemento en un punto futuro” (Basel Committee on Banking Supervision, 2022, pp. 2-3).

En quinto y último lugar, se halla el principio de regulación a prueba de futuro (*future-proof regulation*). Este principio consiste en regular de forma abierta, de tal modo que la evolución de distintas opciones, negocios, tecnologías o incluso incidentes no exijan cambios inmediatos en la regulación. Básicamente, busca ver el potencial a largo plazo y resaltar la existencia de una amplia variedad de opciones heterogéneas debido a la incertidumbre de la evolución de la materia tratada. En ese sentido, la regulación debe contener una formulación ágil capaz de adaptarse a cambios (OECD iLibrary, 2020, pp. 1-131).

La clave de este tipo de solución, que parece ser la más factible, es el hecho de que la regulación europea hasta el momento se ha diseñado con alto nivel de detalle, por lo que el sector privado y los supervisores están acostumbrados a operar a partir de reglas y no de principios, lo que implicaría una mayor interacción público-privada para aclarar expectativas de ambas partes o problemáticas que se puedan presentar.

Únicamente en aquellos casos en los que se identifique una nueva funcionalidad o una alteración significativa en los riesgos de la operativa, se debería considerar una regulación *ex novo*. Los criptoactivos y las DeFi son precisamente el tipo de actividad que requeriría una regulación específica, puesto que cumplen con los criterios establecidos por Amstad en 2019. Estos criterios incluyen: (i) basarse en tecnología *Blockchain* disruptiva que plantea nuevas problemáticas (por ejemplo, la aparición de bifurcaciones de *Blockchains* existentes), (ii) combinar nuevos modelos de negocio y/o ámbitos geográficos, y (iii) enfrentar nuevos riesgos operacionales derivados de la digitalización.

### **III. LA APLICACIÓN DE LA ANALOGÍA EN *FINTECH***

#### **1. Planteamiento**

Las lagunas normativas o jurídicas son definidas por el diccionario de la Real Academia Española (RAE) como la “inexistencia de regulación para un supuesto de hecho, que no ha sido contemplado por el ordenamiento”. Por tanto, como indicó Aguiló (2021), las lagunas jurídicas se entienden como un “defecto o carencia”, careciendo de un sentido positivo (p. 17). Las lagunas también pueden definirse como “un hueco o vacío normativo, la inexistencia de una norma allí donde se esperaba tenerla” (Rodilla, 2014, p. 341) o como “la ausencia de regulación de una determinada situación que exige respuesta por parte del Derecho” (Segura, 1989, p. 289).



La primera pregunta que debe plantearse es si realmente existen o se puede hablar de lagunas jurídicas. Ello se debe a que numerosas teorías del derecho parten del presupuesto de que el ordenamiento jurídico es pleno y cerrado (aquellos aspectos no contemplados en la norma serán integrados por los jueces) (Bobbio, 2016, pp. 201-229). Estos, a su vez, deberán resolver basándose en el derecho supletorio (regulación aplicable por defecto), en las interpretaciones extensivas de la norma (cubriendo escenarios inicialmente no previstos), en la aplicación de analogía (en estos casos, el juez está creando *de facto* normativa y sentando tendencias jurisprudenciales) o acudiendo a las fuentes del derecho.

El ordenamiento jurídico se considera completo y aquellas “hechos, actos o relaciones que deja sin regular deben considerarse irrelevantes jurídicamente, puesto que quedan fuera de los límites de su ordenamiento” (Ramos, 2017, p. 49). En contraste con esta afirmación, Laurenz (2001) sostuvo que “una norma jurídica, que primero ha de ser creada, no existe todavía” (p. 398), lo que implica que tanto la ley como el ordenamiento jurídico adolecen de lagunas. El juez, al interpretar y actuar como legislador, está reconociendo la existencia de lagunas en el ordenamiento jurídico (Segura, 1989, p. 300). La posición de esta tesis concuerda con esta postura, cuyas argumentaciones pueden identificarse a continuación.

Son precisamente innovaciones como los casos de *FinTech*, las que demuestran que esta posición no puede considerarse correcta, puesto que pueden existir adelantos tecnológicos con un impacto material en la industria financiera, la estabilidad de los mercados y los consumidores que, debido a la rapidez de los cambios, no están reguladas. Esto no implica que sean irrelevantes jurídicamente, sino que, debido a su novedad, no hay referencias normativas o jurisprudencia a las que se pueda acudir (este sería el caso de la aplicación de API o *Blockchain* en el procesamiento de pagos, como se ha visto en el contexto de las *PayTech*).

A este tipo de lagunas, en las que la norma se vuelve incompleta después de su emisión debido a la alteración de los supuestos de hecho o figuras en las que se basaba, se les denomina “lagunas secundarias” (Segura, 1989, p. 305). Conviene citar las palabras de Engisch (1967) como ejemplo de este tipo de situaciones:

*Esto es aplicable, tanto al cambio de valoraciones como al cambio de circunstancias de hecho con respecto al objeto de la regulación; no pocas veces se producen lagunas en la regulación jurídica a posteriori cuando debido a*

*fenómenos económicos (inflación) o progresos tecnológicos (...) se plantean problemas jurídicos para los que la regulación existente hasta el momento no proporciona ninguna solución satisfactoria.* (Engisch, 1967, p. 1)

En contraste con las lagunas secundarias, existen las lagunas primarias, en las que se da una ausencia de normativa que posteriormente se constata en el proceso de aplicación del derecho o en la vida práctica (Segura, 1989, p. 305). Estas lagunas primarias podrían diferenciarse, a su vez, entre voluntarias (omisión intencional) o involuntarias (omisión no buscada).

Se podría considerar que este tipo de lagunas primarias voluntarias se daría en la regulación del MiCA mediante la ausencia de referencias a la temática de las DeFi (discutidas en numerosos borradores, por tanto, intencionales) o los contratos inteligentes financieros (no discutidas en los borradores y, por tanto, potencialmente involuntarias). En estos ejemplos, se tratan elementos relevantes hoy en día y, sin embargo, se están dejando fuera del ámbito normativo del MiCA.

De cualquier forma, *FinTech* plantea numerosos casos que sobrepasan los límites de la normativa e incluso, debido al componente de innovación, del ordenamiento jurídico en general. Tal y como indicó Segura (1998), “el resultado final puede quedar fuera en el sentido de crear una norma nueva individual que, en principio, no era previsible que se integrara en el mismo” (p. 302).

Por otro lado, la filosofía del derecho clásica identifica tres tipos de lagunas jurídicas. La primera es la laguna jurídica (ausencia de norma o regulación); la segunda es la laguna axiológica (discrepancia entre lo que el derecho establece y lo que debería reflejar); y la tercera es la laguna técnica, que se produce a raíz de normativas defectuosas (Pérez, 2022, pp. 293-312). A continuación, se identifica cuál de estos tres tipos de lagunas se correspondería con *FinTech*.

Según Bobbio (2016), la laguna jurídica consiste en la “la falta de plenitud consiste en el hecho de que el sistema no tiene una norma que prohíba determinado comportamiento ni una norma que lo permita” (pp. 201-229). Es en estos casos donde, por lo general, los jueces generan interpretaciones normativas con el fin de cubrir aquellas cuestiones no contempladas. En el contexto de las lagunas jurídicas, la cuestión es si dicha ausencia de normativa implica a) irrelevancia o b) relevancia (a modo de exclusión o a modo de inclusión).

a) Irrelevancia (espacio jurídico vacío)<sup>135</sup>: la irrelevancia de lo no regulado es motivada por Bobbio de la siguiente manera: “Lo jurídicamente irrelevante es en realidad lo mismo que el permiso jurídico [...], al ser el permiso también una forma de regulación, el pretendido espacio jurídico vacío es en realidad es una parte del espacio jurídico pleno” (Pérez, 2022, p. 304).

Por tanto, no existen lagunas, sino espacios irrelevantes (vacíos). En este caso, no se puede estar de acuerdo con este enunciado, puesto que, como se argumentó anteriormente, la normativa evoluciona o se genera debido a la presencia de realidades relevantes no recogidas por la norma (de inicio o devenidas con posterioridad). El mero hecho de que existan revisiones de las normas muestra que pueden existir hechos relevantes no contemplados normativamente. La generación de normativas *ex novo* ante cambios de paradigma (por ejemplo, la innovación tecnológica) tampoco podría soportar esta teoría de la irrelevancia de los comportamientos no contemplados por la norma, dado que, aunque sea en periodos transitorios, desde el nacimiento de la actividad en la realidad hasta la delimitación normativa, se dan espacios temporales de alegalidad de las actividades relevantes. Al respecto, Segura (1989) señaló que “no es posible hacer una separación tan tajante entre lo jurídicamente relevante y lo indiferente al Derecho” (p. 291).

b) Relevancia de los hechos no recogidos en la norma: este criterio se aplica con base en lo que Zitelmann denominó “norma general negativa” o “norma general exclusiva” por la que existen normas implícitas<sup>136</sup>. Es decir, existe una norma general sobreentendida por la que lo que no está contenido (limitado) por la norma, está libre de castigo. En otras palabras, se habla de una dialéctica de opuestos por la que:

*Si se promulga una norma particular es para establecer una prescripción que antes no existía, y puesto que toda norma particular es una excepción a la general, el contenido de esta norma particular debe ser, entonces, contrario a la norma general.* (Pérez, 2022, p. 305)

---

<sup>135</sup> El representante por excelencia de la doctrina del espacio jurídico vacío (irrelevante) es Karl Bergbohm. Según esta teoría, existen dos esferas o espacios: aquella sometida al derecho y, por tanto, completa; y la esfera intencionalmente no contemplada en el derecho, por ser indiferente a este o irrelevante (fuera de ámbito). Por consiguiente, esta teoría concluye que no hay lagunas, puesto que todo lo relevante está incluido en el derecho (Segura, 1989, p.290).

<sup>136</sup> De acuerdo con Segura (1989), la teoría de la norma general exclusiva es defendida por Zitelmann, Donati y Kelsen. El autor indicó que “se parte, pues, de la existencia de una norma que está presente en todo sistema jurídico y cuyo tenor sería el siguiente: todo lo que no está expresamente prohibido, ordenado o sancionado, está jurídicamente permitido” (Segura, 1989, p. 293).

Según este principio, las normativas bancarias y financieras vienen a limitar o prohibir, siendo la regla general que todo lo que no esté contenido (limitado en ellas) sería permisible, por lo que las actividades *FinTech* no contempladas (limitadas) en la normativa serían actividades permitidas. De acuerdo con este punto de vista, no existen lagunas, dado que no hay nada fuera del derecho, sino que todo está cubierto por la norma general. Este tipo de razonamiento es más propio del derecho penal (normas negativas por excelencia) que del derecho bancario.

Por otro lado, Bobbio propuso una “norma general inclusiva” para las actividades no reguladas expresamente. De esa manera, la norma particular se expone como una concreción o particularización de la actividad (Pérez, 2022, p. 306). Según este principio, las normas bancarias y financieras vendrían a especificar ciertos requerimientos o casos, mientras que las actividades *FinTech* no contempladas estarían permitidas.

El segundo tipo de laguna se refiere a la “mera disonancia entre lo que el derecho dice y lo que debería, a juicio de cada uno, decir” (Pérez, 2022, pp. 293-312). Según Rodríguez (1999), “se produciría cuando, pese a la existencia en el sistema jurídico de referencia de una solución para cierto caso, tal solución es considerada axiológicamente inadecuada debido a que la autoridad normativa no ha tomado como relevante cierta distinción que debería haber sido tomada en cuenta” (p. 349). No se trata de que no exista solución legal, sino que esta resulta no idónea (Zitelmann la llegó a calificar de repugnante) (Zitelmann, 1922, pp. 540-559). En ese orden de ideas, las normas pueden resolver el supuesto de hecho que se plantea, pero ignorando un elemento relevante y, por tanto, ofreciendo una solución no adecuada o deseada (por ejemplo, aplicando a más de lo que debería). Estos casos no serían el principal desencadenante para la normativa *FinTech*, puesto que gran parte aún no está contemplada. Sin embargo, podría considerarse que, en el caso de DORA, un ámbito de aplicación tan extenso recoge contrapartes heterogéneas, pudiendo resultar en soluciones sobrecargadas para determinadas contrapartes (por ejemplo, proveedores de soluciones *RegTech*)<sup>137</sup>.

Finalmente, las lagunas técnicas se generan al establecer normas defectuosas que impiden una aplicación efectiva por falta de algún elemento que el juez deberá completar. Similar al caso anterior, debido a que se trata de una actividad joven aún, no existen una

---

<sup>137</sup> Esta problemática se expone en el apartado V, “AD-HOC MODEL OF OPERATIONAL RESILIENCE IN EUROPE: DORA”.

multitud de casos que hayan llegado a tribunales, por lo que la probabilidad de detección de lagunas técnicas todavía es baja.

En conclusión, se identifica que el primer foco o tipo de lagunas que se daría en la actividad *FinTech* es de tipo jurídico. Se podría abrir un inciso para considerar si se puede dar un choque de normativas por exceso de regulación (por ejemplo, entre MiCA, PSD II y MiFID II). En estos casos, no se hablaría de lagunas, sino de antinomias (incoherencias de las piezas normativas). Ejemplos de este riesgo se exponen en el capítulo de análisis de las principales iniciativas regulatorias *FinTech*.

Respecto a cómo solventar las lagunas jurídicas (supuestos de hecho o actividades materiales o de relevancia, no contemplados), la solución a largo plazo sería la de proceder al desarrollo de normativa que resuelva la cuestión cuando esta haya adquirido materialidad suficiente. Sin embargo, en el periodo transitorio, los jueces y tribunales están obligados a resolver todas aquellas cuestiones que se les planteen, mediante la interpretación del ordenamiento jurídico existente (aplicación de analogía<sup>138</sup>).

La acepción viene de los términos griegos *ana logon* (de acuerdo con la lógica o correspondiente con la *ratio*) (Macagno y Walton, 2009, pp. 154-182). El razonamiento analógico se emplea para ofrecer soluciones en aquellos casos en los que se produce un vacío entre los hechos y la normas, empleando reglas generales a situaciones que no estarían directamente dentro de su ámbito de aplicación (Weinreb, 2005, p. 92).

Por su parte, Macagno y Walton identificaron tres consideraciones clave respecto a esta figura: (i) la analogía es una conclusión que se sigue de dos premisas por medio de una inferencia silogística; (ii) la analogía es una inferencia de una premisa particular a una conclusión particular, por medio de un razonamiento que no puede clasificarse como deductivo o inductivo; y (iii) la analogía es un tipo de razonamiento imperfecto, que lleva a conclusiones presuntivas. La analogía viene siendo aplicada por el Tribunal Supremo como solución desde hace mucho tiempo (existen referencias en sentencias de 1911). Vallet de Goytiloso (1995) tomó las palabras de Castan Tobeñas (expresidente del Tribunal Supremo), quien afirmó que “El Tribunal Supremo acepta sin escrúpulo el

---

<sup>138</sup> La analogía ya la venían aplicando los jurisconsultos y los pretores para completar acciones civiles, creando, mediante edicto, otros medios jurídicos análogos (Vallet de Goytisoló, 1995, p. 1045). Para Vallet de Goytisoló (1995), “dado el realismo de los juristas romanos, la analogía que ellos empleaban se fundamentaba en una *ratio* de similitud de justicia o de utilidad entre el caso ya regulado y el caso objeto de examen”.

procedimiento analógico, aplicándolo como principio de derecho a través del axioma de que “donde existe la misma razón de ser, idéntica la regla aplicable”” (p. 1081).

Dentro de las soluciones de analogía caben dos tipos: la analogía *de legis* y la analogía *de iuris*. La analogía *de legis* consiste en aplicar la ley a un supuesto no contemplado en esta, pero similar (la ley aplica porque la sustancia de la actividad es equivalente). La analogía *de iuris*, sin embargo, se presenta cuando el ordenamiento jurídico en su totalidad (es decir, no solo las normas, sino también otras fuentes del derecho) se aplica a una situación similar a otras ya contempladas (Salguero, 2017, pp. 101-128). Es decir, la analogía *de iuris* es una forma de obtención y aplicación de los principios generales del derecho.

En la coyuntura de las actividades *FinTech*, la solución a corto plazo sería una interpretación extensiva de lo ya existente o de casos similares, es decir, la aplicación de la analogía. En este sentido, para *FinTech* específicamente, la respuesta se ha resumido en la frase “*same activity, same risk, same rules*”. A continuación, se analizan las implicaciones de este principio y si realmente puede ser una solución total a la cuestión de ausencia de regulación en *FinTech*, puesto que descansa sobre una lógica en la cual el razonamiento tendría la misma solidez que el más débil de sus eslabones o fases<sup>139</sup>.

## **2. Analogía en *FinTech*: misma actividad, mismos riesgos, mismas reglas**

Como se mencionó anteriormente, esta frase (*same activity, same risk, same rules*) ha estado en boca de numerosas autoridades y académicos con la finalidad de justificar la extensión de los marcos regulatorios existentes a la actividad *FinTech* (Lautenschläger, 2017, pp. 1-3; Hoyler, 2022, pp. 1-2; European Banking Federation [EBF], 2022b, pp. 1-24; Wuermeling, 2022, pp. 1-7). Solo en el contexto del regulador inglés esta correlación se enfoca únicamente en el componente del riesgo, y no en el de actividad, tal y como dejó en evidencia en sus publicaciones (UK HM Treasury, 2022, p. 15). En virtud de ello, se considera un pilar fundamental a la hora de afrontar los retos de las nuevas tecnologías en finanzas.

Los supervisores parecen establecer la lógica de “si-entonces”, por la cual se dan dos premisas: misma actividad, mismo riesgo. Si ambas se alcanzan, entonces se aplicaría la misma norma mediante el criterio de analogía y equidad. Sin embargo, es necesario

---

<sup>139</sup> Esta sería la base del enunciado deductivo o de encadenamiento de ideas de Descartes (Vallet de Goytisolo, 1995, p. 1087).

analizar de manera crítica si realmente se trata de la misma actividad y los mismos riesgos, puesto que el criterio de analogía normativa solo debe aplicarse cuando existen condiciones de analogía en el hecho (Sánchez, 2019, pp. 169-170).

La frase de análisis se puede dividir en dos partes según los principios de la hermenéutica: un primer elemento de juicio fáctico que abarca los componentes de actividad y riesgo, y un segundo elemento de juicio lógico en el que, al existir una identidad de razón, se concluye que la solución normativa es adecuada (“mismas reglas”) (Sánchez, 2019, pp. 169-170).

### ***2.1 Juicio fáctico de la misma actividad***

Para analizar si *FinTech* es equivalente a las actividades reguladas, es necesario identificar cuáles son las actividades reguladas en la actualidad. Esto supone un cambio de orientación en cierta medida en comparación con el enfoque de supervisión basado en las entidades. A modo de ejemplo, la página web del Banco de España, al momento de detallar su mandato supervisor, hace referencia a lo siguiente:

*[...] la solvencia y el cumplimiento de la normativa específica de los bancos, las cajas de ahorros, las cooperativas de crédito, las sucursales de entidades de crédito extranjeras, los establecimientos financieros de crédito, las entidades emisoras de dinero electrónico, las sociedades de garantía recíproca y de reafianzamiento, los establecimientos de cambio de moneda y las sociedades de tasación. En el caso de las sucursales de entidades de países de la Unión Europea (UE), sus facultades se limitan al control de la liquidez de la sucursal y del cumplimiento de las normas de interés general. (Banco de España, 2022, p. 1)*

Dicho de otro modo, el enfoque actual, en cierta medida, se centra en determinados tipos de entidades que se han catalogado en función de sus objetos sociales, siendo estas actividades reservadas. Esta aproximación es heredada de las metodologías regulatorias originarias (*entity-based*) que ya se aplicaron al abordar el Mecanismo Único de Supervisión.

En consecuencia, se puede hablar de dos niveles en la actualidad: un nivel primario, centrado en determinados tipos de entidades, y un nivel secundario, que se refiere a la

actividad u objeto subyacente que es el que realmente cualifica a la entidad para tener el calificativo correspondiente (por ejemplo, sociedad de valores).

Al analizar la actividad *FinTech*, se pueden identificar, en primer lugar, modelos equivalentes a actividades actuales (por ejemplo, operaciones de pago o billeteras digitales). En segundo lugar, modelos que son una extensión de actividades supervisadas (este sería el caso del *social trading* al considerarse una reinterpretación de la actividad de asesoramiento en inversiones). Y, en tercer lugar, actividades nuevas, como las operaciones con criptodivisas, puesto que el fundamento subyacente difiere sustancialmente de las divisas de curso legal. Esta interpretación extensiva se basaría en una interpretación principalmente teleológica de las normas, que parece adoptarse para intentar abarcar el fenómeno *FinTech* dentro de los límites ya establecidos.

Las actividades que son sustancialmente iguales y aquellas que podrían considerarse similares mediante una extensión o reinterpretación de los términos empleados podrían pasar esta primera criba. Posteriormente se debería analizar si implican los mismos tipos de riesgos o no, para llegar a una conclusión definitiva. Sin embargo, aquellas actividades que no son sustancialmente equivalentes indicarían la necesidad de evaluar la modificación de los marcos regulatorios o el desarrollo de normativas *ad hoc*. Siguiendo el razonamiento, se podría decir que “es distinta actividad *ergo* se aplica distinta norma”.

A modo gráfico, esta situación podría representarse mediante un diagrama de Venn en el que únicamente la intersección de la actividad regulada y la actividad *FinTech* (tanto en sentido estricto como bajo interpretación extensiva) se consideraría como “misma actividad” (ver Figura 51).

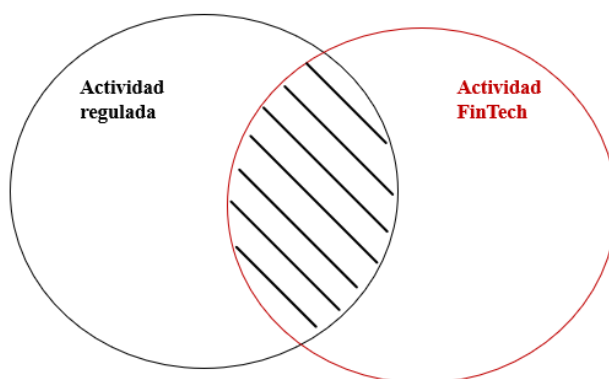


Figura 51. Diagrama de Venn de las actividades reguladas frente a actividades *FinTech*

Nota. Elaboración propia.



El enfoque subyacente de regulación basada en la entidad debería ser secundario y propio de requisitos prudenciales, tal y como se viene aplicando en la metodología regulatoria. Por ello, si en la actualidad existen requisitos especiales de capital, solvencia, liquidez y colchones de estos para las entidades financieras catalogadas como sistémicas (G-SIB) (Borio et al., 2022, pp. 1-8), se consideraría adecuado tomar un enfoque similar en el mundo *FinTech*, lo que se traduce en requisitos del mismo tipo para entidades que presenten riesgos del mismo tipo como pueden ser las *BigTech* o aquellas entidades emisoras de *stablecoins* sistémicas (identificadas como significativas en MiCA).

En especial, en el supuesto de las *BigTech*, una solución basada en la actividad devendría insuficiente tal y como se observó en el capítulo correspondiente y de acuerdo con la crítica realizada por Borio et al. (2022, pp. 1-8). Por tanto, cabe concluir que el requisito de misma actividad debe incluir un segundo subnivel relacionado con el tipo de entidad a la hora de establecer paralelismos, principalmente en aspectos prudenciales.

Por otra parte, plantear un enfoque únicamente basado en el tipo de entidad devendría ineficiente con gran rapidez, puesto que los adelantos tecnológicos, como ejemplo *Blockchain*, vienen a desdibujar o reinventar quiénes son precisamente los intermediarios financieros. Por tanto, esta tesis comparte la posición expuesta por Julie Maupin (2017) en su trabajo *Blockchains and the G20: building and inclusive, transparent and accountable digital economy*, que puede dibujarse en el siguiente párrafo:

[...] *Blockchains also introduce grave new risks to the global economy by displacing or bypassing some of the intermediaries upon whom governments have historically relied on to implement important regulatory safeguards. It is not yet clear how safeguards such as the Basel provisions promoting financial system stability or the Financial Action Task Force rules combatting tax evasion, money laundering, terrorist financing and other Dark Web activities can be implemented in a Blockchain-powered world.* (Maupin, 2017, p. 3)

## **2.2 Juicio fáctico de mismo riesgo**

Similar al caso de las actividades, los riesgos que presentan las actividades *FinTech* en comparación con los riesgos de las actividades reguladas pueden catalogarse de la siguiente manera: (i) aquellos riesgos que disminuyen en comparación con los modelos conocidos (por ejemplo, el riesgo de falsedad de una transacción en *Blockchain* se reduce drásticamente), (ii) aquellos que son sustancialmente equivalentes a los modelos

tradicionales (la identificación de clientes por canal remoto es equivalente en una banca digital y en un modelo de neobanco) y (iii) aquellos riesgos que aumentan en comparación con lo contemplado (en este caso, podrían encajar las plataformas de negociación descentralizadas).

Asimismo, podría dibujarse de nuevo un diagrama de Venn, puesto que únicamente aquellos riesgos que se consideren equivalentes o extensivamente equivalentes podrían dar lugar al solapamiento requerido para que se cumplan las premisas establecidas (ver Figura 52).

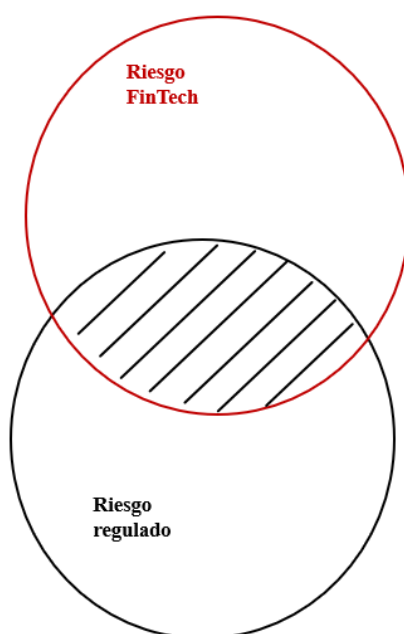


Figura 52. Diagrama de Venn de riesgos regulados frente a riesgos FinTech

Nota. Elaboración propia.

Sin embargo, el alto impacto del componente tecnológico hace que, en muchos de los casos, la exposición al riesgo sea sustancialmente distinta a aquellos casos ya contemplados (tanto para entidades financieras reguladas aplicando nuevas tecnologías como para entidades *FinTech* o *TechFin*). Prueba de ello ha sido la aprobación del Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero, también conocido como DORA.

Además, existen otros riesgos inherentes sustancialmente diferentes, como el riesgo país. Si bien en el mundo tradicional existen criterios de identificación del país que será el regulador y supervisor de cabecera, y aquellos que serán subsidiarios (*home-host country*), en modelos *FinTech* 4.0 plenamente descentralizados, este riesgo se altera,

puesto que no es posible identificar el país cuyas normas y supervisión aplicarán a la actividad en cuestión.

En suma, distinto nivel de riesgo (ya sea inferior o superior) implica distinta norma dentro de este segundo filtro, acumulando así los siguientes elementos fuera de ámbito de la premisa objeto de análisis: distinta actividad, distinto riesgo (mayor o menor).

### **2.3 Juicio lógico de misma norma**

Si se combinan las premisas previamente evaluadas, solo aquellos casos cuya actividad y riesgos sean equivalentes a los de las actividades y los riesgos regulados podrían considerarse como hechos previstos en el espíritu de la norma, lo que llevaría a aplicar la misma solución a través de una intelección normativa o interpretación integradora (Sánchez, 2019, pp. 169-170). Para aquellos casos en que tanto las actividades como los riesgos tienen sustancia propia no idéntica pero similar (extensible), se aplica una creación analógica, dado que, en la práctica, se está creando una nueva norma mediante analogía (Sánchez, 2019, pp. 169-170).

La aplicación de la analogía en *FinTech* parece haber sido la solución temporal aplicada por los supervisores atendiendo a una *ratio iuris* o razón de justicia, que en el ordenamiento jurídico nacional se contempla en el artículo 4.1 del CC<sup>140</sup>. Dicha interpretación solo atendería a aquellos casos de intersección de los planos antes estudiados (ver Figura 53).

---

<sup>140</sup> El artículo 4.1 del CC establece lo siguiente: “Procederá la aplicación analógica de las normas cuando estas no contemplen un supuesto específico, pero regulen otro semejante entre los que se aprecie identidad de razón”.

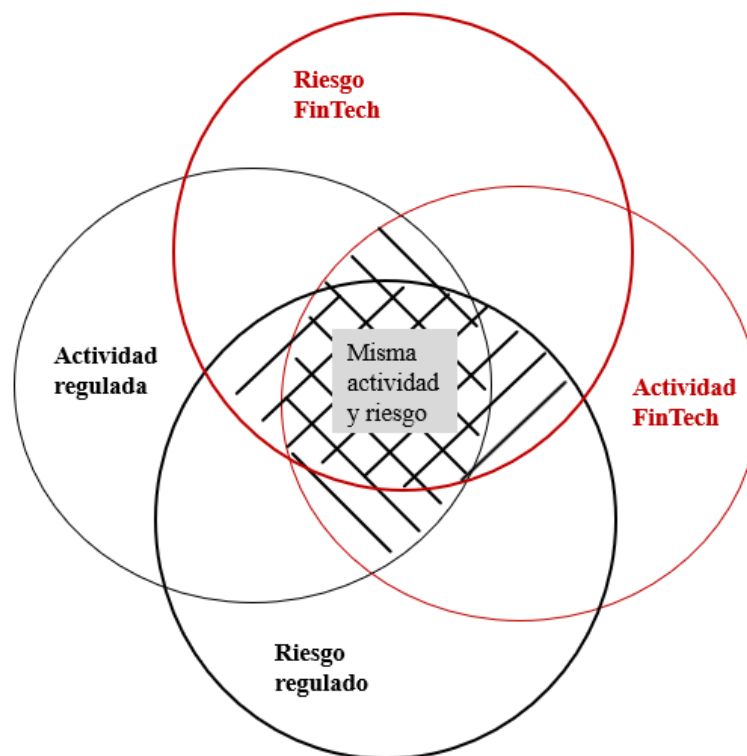


Figura 53. Diagrama de Venn de la aplicación analógica del principio de misma actividad, mismo riesgo, misma norma.

Nota. Elaboración propia.

El artículo 4.1 del CC puede combinarse con otros dos principios generalmente reconocidos en finanzas: proporcionalidad y equidad (Sánchez, 2019, pp. 170-171). Sin embargo, el concepto que se trata incluye no solo el supuesto de hecho de actividad, sino también el de riesgo, por lo que cabe plantearse si el principio de “misma actividad, mismo riesgo, mismos controles” debe contemplarse en la normativa de manera específica, dado que el principio de proporcionalidad como tal es un elemento habitual de la normativa europea.

Tomando como ejemplo las guías de supervisión del BCE, estas reflejan nueve principios de supervisión, entre los cuales están los principios número 3 y 7, de homogeneidad y proporcionalidad (European Central Bank [ECB], 2014, pp. 6-9). En los casos de las principales normativas relacionadas con *FinTech*, se puede contemplar el principio de proporcionalidad explícitamente indicado en todas ellas, dado que, desde el punto de vista técnico, uno de los elementos que se evalúan en las exposiciones de

motivos es la base jurídica de la proporcionalidad de la norma. No solo esto, DORA<sup>141</sup>, en su artículo 28, cuyo título es “Principios generales”, incluye el principio de proporcionalidad, pero pese a que se insiste en el principio de “misma actividad, mismo riesgo, misma norma”, este no se refleja en el proyecto. En el Reglamento Pilot<sup>142</sup> del 30 de mayo de 2022, sí se identifica el principio dentro de su considerando 10, el cual reza de la siguiente manera:

*Al aplicar el presente Reglamento, deben tenerse en cuenta los principios de neutralidad tecnológica, proporcionalidad, igualdad de condiciones y «misma actividad, mismos riesgos, mismas normas» para garantizar que los participantes en el mercado dispongan de un margen regulatorio para innovar y respetar los valores de transparencia, equidad, estabilidad, protección de los inversores, rendición de cuentas e integridad del mercado, y para garantizar la protección de la intimidad y los datos personales, tal como garantizan los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.*

Sin embargo, el principio de proporcionalidad se encuentra explícitamente contemplado en los artículos 8, 9 y 10 del Reglamento Piloto, llegando a usarse la palabra hasta en ocho ocasiones en el documento.

En el terreno de MICA<sup>143</sup>, no existe ninguna mención explícita a ambos principios en el cuerpo del reglamento, pese a que ciertas actividades se asimilan a las de las entidades de emisión de dinero electrónico. Únicamente se tiene en cuenta la proporcionalidad respecto a la evaluación de la base jurídica de la norma.

### **3. En concreto, la posible regulación marco de modelos *FinTech 4.0***

Las finanzas basadas en *Blockchain* presentan características sustancialmente diferentes a las que actualmente están reguladas. Por ejemplo, la irreversibilidad de las transacciones, la capacidad de perdurar en el tiempo incluso más allá de la existencia de sus creadores, y la capacidad de incluir funciones de jueces o árbitros. Una extensión de las estructuras regulatorias existentes por analogía no es una solución satisfactoria a largo

---

<sup>141</sup> Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 y (UE) 2016/1011.

<sup>142</sup> Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo del 30 de mayo de 2022, sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) N° 600/2014 y (UE) N.° 909/2014 y la Directiva 2014/65/UE

plazo, puesto que, como indicó la Reserva Federal estadounidense y refrendó Pablo García Mexía, principios como la nulidad de contratos abusivos o la adaptación a condiciones cambiantes no son compatibles con la lógica de los contratos inteligentes o el acuerdo requerido entre las partes (García, 2018, p. 115).

Por lo tanto, se considera suficientemente fundamentada la necesidad de un nuevo marco jurídico y de derecho, como es el denominado criptoderecho (García, 2018, pp. 97-130) o derecho tecnológico si la tecnología se aborda desde un aspecto más amplio.

Estas regulaciones *ad hoc* tendrían dos capas fundamentalmente: la primera estaría basada en principios y la segunda contaría con un alto contenido técnico. Esto implicaría un adecuado conocimiento de la tecnología, y la legislación. Esto supone, de nuevo, una necesidad de cambio en los miembros de los reguladores y supervisores, dado que el conocimiento jurídico ya no sería suficiente y estos perfiles requerirían de una constante mejora en su dominio de aspectos cada vez más científicos relacionados con las innovaciones tecnológicas (migración hacia una suerte de especialistas en derecho tecnológico).

Como se puede observar, la solución legislativa planteada no es una, sino una combinación de varias, puesto que serían producto de cambios progresivos iniciados por la evolución de la innovación en el mercado. Por tanto, el presente capítulo propone el siguiente proceso normativo para el caso de *FinTech* (ver Figura 51).

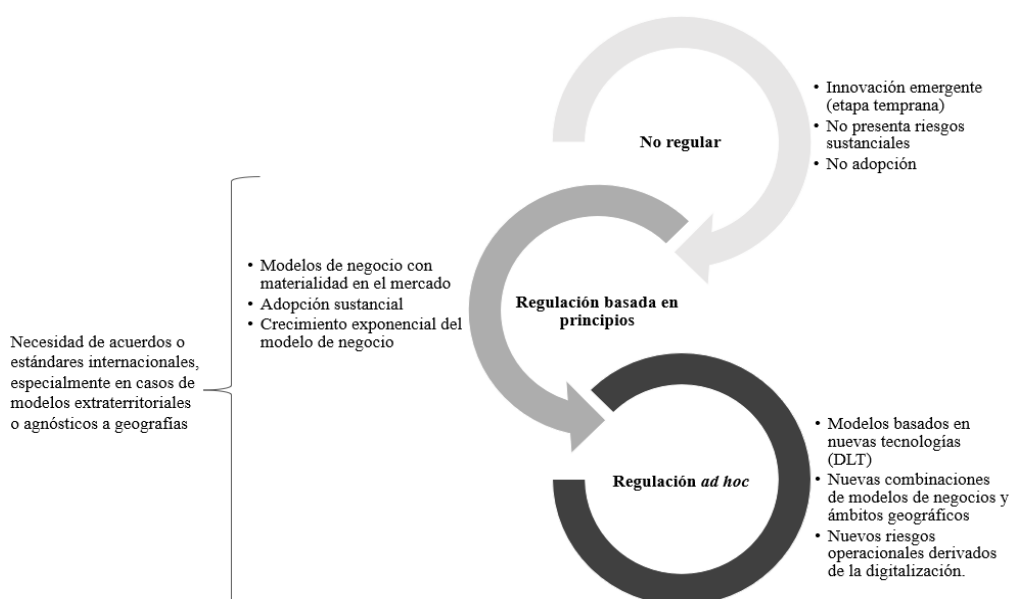


Figura 54. Propuesta del modelo regulatorio FinTech

Nota. Elaboración propia.

## ***2.1 Planteamiento de posibles nuevos regímenes de licencias***

En cuanto a los regímenes de licencias, el considerar estas nuevas empresas como sujetas a supervisión e intentar su encaje en esquemas de licencias existentes puede ser un error, en virtud de que los requerimientos y tiempos que acompañan no serían compatibles con el programa de estos nuevos participantes, convirtiéndose, de este modo, en barreras a su entrada o generando situaciones de inseguridad jurídica.

No debe olvidarse que gran parte de los modelos *FinTech* pueden ser etiquetados como de nicho o especialización. Es decir, resuelven un problema determinado o mejoran un aspecto específico dentro de una actividad históricamente regulada. Por este motivo, los formatos de licencias tradicionales resultarían una sobrecarga para estos modelos de negocio. Se puede tomar como ejemplo los productos de inversión ofertados por proveedores de servicios de criptoactivos.

En la actualidad, se ha interpretado que los productos cripto de inversión deben estar sujetos a la normativa MiFID II. Ello implica, por ejemplo, que la entidad que ofrece dichos servicios deberá adquirir la licencia correspondiente (por ejemplo, de entidad de servicios de inversión, *broker* o custodio, entre otros). Asimismo, el personal encargado del diseño de estos productos o de su oferta deberá formarse y obtener las certificaciones que demuestren que cuenta con los conocimientos necesarios para el desarrollo de estas tareas. Cabe imaginarse que la instrumentación de todos estos pasos implica meses o años, mientras que los productos ya se encuentran operativos en el mercado y ya son contratados por el público en general.

Es precisamente en estos escenarios donde en la actualidad no queda claro cómo proceder o qué soluciones tomar, puesto que los esquemas normativos existentes no se corresponden con las realidades vividas, derivando en situaciones de alejamiento, dado que la actividad no se encuentra ni regulada ni prohibida. Debido al alcance, materialidad y diferenciación con respecto a las actividades conocidas, se puede inferir que muchos elementos derivados de la innovación en finanzas son “otra raza de animal”, lo que requiere un tratamiento y supervisión específicos. Del mismo modo, se necesitarán soluciones de transición o remediación para agentes que ya estaban operando en el mercado amparados por la situación de vacío normativo.

Un segundo ejemplo son los casos de las criptomonedas estables que puedan considerarse equivalentes al dinero electrónico. MiCA establece que, en dichos casos, la

normativa de dinero electrónico sería de aplicación y, por tanto, las entidades que emitan este tipo de *stablecoin* deberían de obtener las licencias de emisión de dinero electrónico. No obstante, la emisión de dinero electrónico no ha resultado atractiva en España (en abril de 2022 solo había nueve EDE de origen español de un total de 270 operativas en la UE) (European Banking Authority [EBA], 2022c).

Adicionalmente, cabe cuestionarse qué solución se adoptará en los casos en los que las *stablecoins* no se encuentren referenciadas con una divisa de curso legal (esto es, si las *stablecoins* están referenciadas en un porcentaje contra la divisa) o aquellos casos en los que, pese a encontrarse referenciada uno a uno, las cantidades de divisa colateralizadas y depositadas en instituciones financieras sean un porcentaje de la divisa (esto es, no el cien por cien, como sucede en el supuesto de emisión de dinero electrónico).

En conclusión, parece que se requiere una mayor dinamización y modernización de los regímenes actuales de licencias en la UE, o bien el desarrollo de nuevos tipos de licencias más ágiles y menos exigentes. Incluso en el caso de los modelos de negocios tradicionales, podrían sopesarse soluciones progresivas que permitieran el inicio de actividades sin imponer requisitos costosos a las entidades que ingresan al mercado (como requisitos de capital escalados o estructurales). Estos requisitos se implementarían gradualmente a medida que el tamaño y el volumen de las operaciones de la entidad aumenten.

Por este motivo, y en una forma similar a los propios modelos *FinTech* con estructura de legos, podría plantearse un esquema de licencias menores o modulares, con la consecuente reducción de exigencias en términos de capital, estructura y, a su vez, tiempos de consecución. Las entidades con una de estas licencias que quisieran diversificar hacia otro tipo de licencias podrían contar con un cierto nivel de homologación de conceptos o tareas a desarrollar para la solicitud de aprobación a las autoridades de las licencias correspondientes a las nuevas actividades.

## ***2.2 Avance de potenciales modelos de regulación supervisora***

En cuanto a los regímenes regulación de supervisión propuestos para los jugadores *FinTech* centralizados, se podría hablar de modelos de supervisión pública directa o indirecta. Esto se traduciría en que aquellas entidades con licencias totales o parciales (modulares), estarían sujetas a supervisión de forma proporcional al riesgo que plantean.



Sin embargo, se reconocería la existencia de entidades *FinTech* fuera del perímetro directo de supervisión.

Para estos casos (*FinTech* no reguladas), puede exponerse una supervisión indirecta o una descentralización de la supervisión. Esto implica que las entidades *FinTech* que sean proveedoras críticas de agentes regulados estarían sujetas a supervisión y auditoría por parte del sector privado regulado. Sus obligaciones relacionadas con el servicio se derivarían de forma indirecta a través de acuerdos contractuales. De esa manera, se produciría una privatización de un rol supervisor, debido a la imposibilidad de este de ofrecer cobertura a nuevas casuísticas que caerían en zonas grises y que podrían no estar mapeadas por este. Esta solución no es nueva, puesto que las funciones de control impuestas en las normativas actuales (auditoría interna, *compliance* y riesgos) obedecen a una suerte de privatización de controles públicos debido a la imposibilidad de supervisar todos los agentes de los mercados. En esta línea, el reglamento de DORA<sup>144</sup> propone controles de las entidades reguladas hacia proveedores de tecnología, entre los cuales podrían encontrarse las empresas de tecnología financiera.

Además, aquellas *FinTech* fuera de perímetros de supervisión pero que establezcan relaciones con entidades reguladas y, por tanto, puedan impactar en el mercado financiero (por ejemplo, proveedores de tecnología), caerían bajo el análisis y escrutinio de las entidades directamente supervisadas, debido a los requerimientos de control de tercerizaciones de servicios materiales o críticos.

---

<sup>144</sup> El análisis crítico del reglamento de DORA se aborda en el apartado “*AD-HOC MODEL OF OPERATIONAL RESILIENCE IN EUROPE: DORA*”.

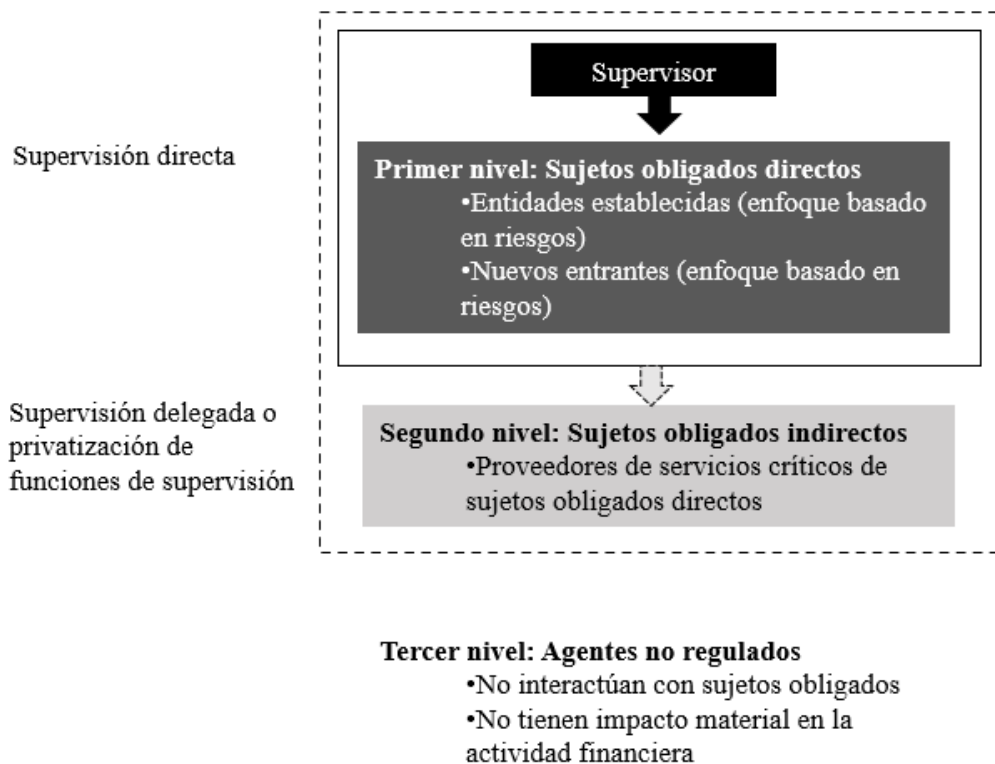


Figura 55. *Propuesta del modelo de supervisión delegada*

Nota. Elaboración propia.

### 2.3 *Ámbito subjetivo, los potenciales nuevos sujetos obligados*

Desde el ángulo regulatorio basado en entidades que prestan servicios financieros, parece que esta solución sería la más adecuada, puesto que seguiría un enfoque basado en riesgos desde el punto de vista de la regulación y supervisión *FinTech*. Sin embargo, en modelos altamente disruptivos, la cuestión de quiénes deben de ser los sujetos obligados puede hacerse más complicada. A modo de ejemplo, de Filippi y Wright (2018) plantearon si los mineros y otras contrapartes necesarias para los modelos de DeFi deberían ser sujetos obligados por la norma. La argumentación se basa en el hecho de que estos funcionan como validadores o jueces, con capacidad de imponer normas en la *Blockchain*. De esa manera, los nodos, mineros o validadores podrían frenar actividades ilegales o llegar a censurar o revertir transacciones (de Filippi y Wright, 2018, p. 187).

Esta lógica no es del todo correcta hoy por hoy, dado que el rol de los protocolos y sus validadores no es otro que el de procesar las transacciones, validando simplemente las reglas o criterios, pero no entrando a evaluar la legalidad de las transacciones u operaciones que están validando. Es decir, estas contrapartes intervienen en la forma, pero

no en el fondo. Si se deseara cambiar este rol, sería posible (se podrían incluir obligaciones básicas, como, por ejemplo, la validación contra listas de sanciones financieras internacionales), pero este tipo de requerimientos deberá contemplarse en una regulación o ley. En el caso europeo, en la actualidad, este tipo de casos no está contemplado.

De manera similar, posibles regulaciones sobre proveedores de servicios de internet podrían potencialmente discriminar entre ordenadores conectados que validan o minan bloques en *Blockchains* que cumplen con las normativas y *Blockchains* que fueran disconformes o *non-compliant* (de Filippi y Wright, 2018, p. 179). Sin embargo, debido a su potencial tinte de censura, este tipo de soluciones deberían considerarse bajo criterios de requerimientos mínimos globalmente aceptados.

Un tercer grupo de potenciales nuevos sujetos obligados serían los desarrolladores (de Filippi y Wright, 2018, pp. 179-183), dado que son estos quienes orquestan y despliegan los nuevos modelos financieros a través de contratos inteligentes y códigos. Sin embargo, hasta ahora no cuentan con un régimen de responsabilidad claro, ni pueden identificarse en todos los casos. Este parece ser uno de los caminos tomados por los tribunales durante 2022, cuando el supervisor americano (OFAC) incluyó a Tornado Cash en la lista de sanciones estadounidenses. Tornado Cash era una solución empleada para fines de privacidad que venía siendo utilizada para actividades criminales, puesto que permitía romper con la trazabilidad de las operaciones realizadas por las partes (a este tipo de operativa se la denomina *tumbling* o *mixing*). Tras la decisión, los tribunales holandeses procedieron a imputar al desarrollador de la solución, incluyendo cárcel preventiva a la espera de juicio (Guerrera, 2022, p. 1).

No obstante, este enfoque presenta limitaciones significativas. En primer lugar, resulta complicado discernir cuándo un desarrollo se realiza con la intención de incumplir normativas o no. Puede haber situaciones en las que un desarrollador diseñe y despliegue un contrato inteligente con una finalidad legítima, pero luego este sea utilizado de manera ilícita. Un modelo de responsabilidad objetiva ampliaría la carga en cualquier escenario, lo que desincentivaría el desarrollo de la innovación y podría tener resultados no deseados.

La segunda limitación, que se ha abordado ampliamente a lo largo de este trabajo, es el hecho de que estas imposiciones solo podrían llevarse a cabo dentro de los límites

autoridad jurisdiccional (de Filippi y Wright, 2018, pp. 179-183). Esto podría resultar en que los desarrolladores busquen jurisdicciones con niveles de responsabilidad más bajos o la ausencia de tales obligaciones.

Como se puede observar, existen colectivos de sujetos no contemplados hasta ahora en la regulación europea y que podrían regularse de diversas formas en los próximos años. No parece existir una solución óptima, por lo que una combinación de medidas sería lo más adecuado, teniendo en cuenta los principios de enfoque basado en riesgos y proporcionalidad. En el caso de regular a estas nuevas contrapartes, se deberían establecer estándares mínimos para garantizar una viabilidad adecuada y el progreso de la innovación tecnológica.

### **3. Recapitulación**

En conclusión, pese a que este principio parece ser clave para la interpretación analógica normativa del fenómeno *FinTech* en Europa, no está específicamente contemplado en los marcos normativos recientemente aprobados o en desarrollo, ni en las guías de supervisión del BCE, por lo que no existe sustento jurídico explícito para su aplicación. Esto no sucede en casos como el del principio de proporcionalidad, como se evidenció. En consecuencia, la aplicación práctica del principio se basaría en un criterio finalista, empleando para ello la analogía. De esa manera, como argumentó Thomas Hobbes en el *Leviatán*, “el intérprete se transforma en legislador”, pudiendo existir el riesgo de cambiar el auténtico sentido originario de la norma (Robles, 2015, p. 409).

Por otro lado, el empleo de la analogía parte de la aplicación de esta dentro de unos parámetros establecidos, esto es, en un ordenamiento jurídico concreto en el que se evalúa si la actividad o el sujeto se interpretan como contenidos en la norma. En el caso de las actividades *FinTech*, el núcleo del problema reside en su carácter global en muchos casos, por lo que cabe preguntarse si el supervisor sería el que tendría la capacidad de identificarse como supervisor de cabecera y, por tanto, base del criterio para juzgar si la actividad es equivalente a actividades reguladas de la jurisdicción. Del mismo modo, puede cuestionarse cuál sería esa “misma regla”, pudiendo ser múltiples para actividades internacionales y, en el concreto caso de *FinTech*, identificando vacíos legales y de supervisión a la hora de llevar a cabo sus operativas.

Si bien un supervisor local puede interpretar y resolver las cuestiones abiertas mediante el uso de la analogía y acudiendo a los principios generales del derecho, estas soluciones estarían limitadas a la actividad en la jurisdicción o con respecto a los nacionales de esta, pero no resultaría completa al no poder aplicar en el resto de las jurisdicciones o al resto de individuos no nacionales. Por esta razón, la comunidad internacional debería acordar unos principios mínimos para actuar y regular en esta materia, tal y como se expone en el capítulo de conclusión.



## **CHAPTER VII. CRITICAL ASSESSMENT OF SPECIFIC REGULATORY INITIATIVES**

This part evaluates whether the principles and criteria established in the former section are considered during the development of regulatory initiatives. For this purpose, the chapter is structured as follows. First, a high-level overview of the global proposals of organisations such as the Financial Action Task Force is provided. Second, the source of the European regulatory framework for *FinTech* is identified, with the 2018 *FinTech* Action Plan and the 2020 Digital Finance Strategy for the EU as its bedrocks. Then, a critical analysis of the key regulatory proposals of the EU in the *FinTech* arena is provided. This assessment distinguishes between ad hoc regulations and amendments of existing frameworks. Among the ad hoc models are MiCA (Markets in Crypto Assets), the DLT Pilot Regime, and the Operational Resilience act. These regulations are specific to the financial sector. The Digital Markets Act and the Digital Services Act are also interpreted as ad hoc regulations; however, these are not *FinTech* specific but transversal to any industry.

Finally, the review of existing rules impacted by the *FinTech* space is contemplated via eIDAS 2 and a potential PSD III.

### **I. GLOBAL INITIATIVES**

This section begins by noting that, presently, the focus of regulatory efforts and coordination between supervisors has been around cryptocurrencies, and the greatest progress seems to be in the area of financial crime.

This is due to the coordinating efforts of the Financial Action Task Force (FATF). Although the FATF is an international body that issues guidelines and standards, these are, *de facto*, the starting point for the development of legislative initiatives by member jurisdictions. In addition, this body has a mechanism in place to evaluate the levels of progress made by member countries with respect to its guidelines and standards, which is published, and is therefore a tool for aligning strategies in this area.

The FATF has issued numerous reports on crypto assets and has amended its pillar document (the recommendations) to provide guidance on how to manage the risk they

pose (FATF, 2012). The following are the main FATF reports generated up to 2021 on crypto assets:

- (FATF, 2012). International standards on combating money laundering and the financing terrorism and proliferation. The FATF recommendations.
- (FATF, 2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. FATF Report.
- (FATF, 2015). Guidance for a Risk-Based Approach. Virtual Currencies.
- (FATF, 2020). FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins.
- (FATF, 2020). 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs.
- (FATF, 2021b). Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs.
- (FATF, 2021c). Virtual Assets and Virtual Services Providers.
- (FATF, 2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
- (FATF, 2023). Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

These guidelines are focused on virtual assets, virtual service providers, and points of exchange of official currency for cryptocurrency and vice versa (also known as on-ramps and off-ramps). However, recent reports have extended the scope of control suggestions to other counterparties.

With the identification of distributed ledger technology as a new form of value transfer, the FATF recommended that its members extend this requirement to cryptocurrency transactions, calling for action and requesting regulatory changes regarding financial crime to bring crypto assets service providers within the scope of authorities' supervision.

The FATF also recognises that it is currently difficult to control elements concerning decentralised finance or decentralised crypto assets (FATF, 2021b, p. 33). The situation is aggravated by the fact that the DeFi world is constantly changing,



which means that the FATF is in the process of updating its guidelines on the subject, and many jurisdictions have not yet developed any regulations based on the first guidelines issued by the FATF (2021b, p. 33).

One of the elements of interest is the so-called travel rule and its application to the crypto world. The travel rule refers to FATF Recommendation 16, whereby financial institutions are obliged to include certain payer and payee details in transfer orders as well as keep them throughout the financial system institutions involved; in this way, they can check the details against sanctions or anti-money laundering lists (FATF, 2021b, p. 77).

In its 2020 status review document, the FATF indicated that the rule was implemented only in part of the membership and not in its entirety. Furthermore, it highlighted the fact that the private sector, while developing solutions to address this new rule, had not yet arrived at a scalable or standardised solution (FATF, 2020a, p. 2). The implications of the non-application of the travel rule by Member States has been previously addressed as part of the supervisory gap theory.

The partial implementation of the standard also generated another problem that was difficult to solve: in the case of crypto transactions managed by one crypto service provider in a country where the standard applied and another provider in a country where the standard had not yet been published, it was not clear what measures, responsibilities, or how to proceed. This situation has been referred to as a sunrise issue (FATF, 2020a, pp. 17-18).

In its second review in 2021, the FATF was concerned that, two years later, half of its members still had not modified their local regulations and, as a result, the requirements regarding the information that must accompany cryptocurrency transactions remained ineffective. This discouraged private investment in technological solutions to perform this type of task in relation to transactions carried out in distributed ledger technology, which, by design, lacks the possibility of including this type of information in its blocks (FATF, 2021b, p. 2). For this reason, to force countries to implement its standards, the FATF has opted to update its standards 'FATF Recommendations' document, which is a *de facto* mandatory guide for its members.

The International Organization of Securities Commissions (IOSCO), for its part, has focused its efforts on highlighting the risks of crypto assets, making references to

decentralised platforms in its February 2020 report *Issues, Risks and Regulatory Considerations Relating to Crypto asset Trading Platforms*.

In contrast, the Bank of International Settlements (BIS) has geared its resources towards the analysis of central banks' *stablecoins* and digital currencies, promoting the progress of projects on the latter. Regarding decentralised finance, in December 2021 its quarterly review included a document entitled *Defi Risks and the Decentralisation Illusion*, which proposed an approach to the risks of decentralised finance (Aramonte et al., 2021, p. 27).

Finally, the Basel Committee on Banking Supervision issued a report in December 2022 regarding the prudential treatment of crypto assets, classifying tokenised and *Stablecoin* assets into one group (group 1.a and 1.b) and assigning remaining crypto assets to group 2. This classification has implications for financial institutions' provision of capital resources, which would be subject to certain maximum limitations. The proposal was initially controversial because the use of technology based on distributed registries implied a capital surcharge, which extended not only to crypto assets but also to the tokenisation of financial instruments, discouraging innovation in this area, which from a compliance point of view is less risky than cryptocurrencies. Moreover, this measure disincentivises the banking sector from having these kinds of exposures and thus from exploring possible uses of this technology, leaving it to non-regulated actors.

In practice, this could mean that while non-regulated, inexperienced actors advance experimenting with technology and rendering services to clients, regulated actors with healthier control frameworks would be penalised if rendering the same types of services even though they would potentially be in a better position to control new risks.

The main reason behind this limitation would be to avoid possible ripple effects from the crypto industry into the real financial ecosystem via its institutions. However, this measure would not have followed the technology-neutral principle previously identified. The December 2022 version of the report has taken a flexible approach.

## **II. EUROPEAN FRAMEWORK**

The European Digital Finance Package published in 2020 (Comisión Europea, 2020) has its precedent in the *FinTech* Action plan communication issued on March 8<sup>th</sup>, 2018 (European Commission, 2018, pp. 1-18). Both cases aim to map the

innovations impacting the financial sector with the purpose of setting up a project plan on how to manage them from the regulatory and supervisory perspectives.

Both documents are the origin of several core regulatory initiatives that will be analysed from a critical perspective in this chapter. There are specific regulations (such as the crowdfunding one or the AML related) that have been previously analysed and therefore, will not be included in this chapter. However, both ad-hoc regulations -MiCA, DLT Pilot, DORA as directly financial related, and DMA and DSA as transversal – have their origins in the *FinTech* Action Plan and the Digital Financial Strategy for the EU. Something similar happens with the review of certain regulations such as PSD II and eIDAS 2. For this reason, a brief overview of both *FinTech* Action plan and the European Digital Finance Package should be made as a starting point.

### **1. *FinTech* Action Plan of 2018**

The 2018 *FinTech* Action Plan sets out three main objectives at the European level from the financial sector perspective: (i) to enable innovative business models to reach EU scale, (ii) to support the uptake of technological innovation, and (iii) to enhance security and resilience.

In this way, the European Union aims to establish an adequate regulatory and supervisory framework to drive innovations in the region. The regulatory certainty the framework provides can protect consumers' and investors' interests and market stability (Barrio, 2021, pp. 59-60). As Tapia Hermida highlighted, the rapid advance of *FinTech* has triggered structural changes in the financial sector. The *FinTech* Action Plan seeks a regulatory balance between excessively prescriptive regulation and abstention from regulating, which would create financial instability and insecurity (Tapia, 2020, p. 543).

The three main objectives in the action plan and their analysis prompted the European Commission to develop a series of tasks to be performed in successive years. The status of these tasks as of 2022 is presented in Table 12.

<b>FinTech Action Plan Objectives (2018)</b>	<b>Topic</b>	<b>Action taken as of 2022</b>
Enabling innovative business models to reach EU scale	Licensing requirements for <i>FinTech</i> firms	<i>Crowdfunding</i> Regulation (Regulation (EU) 2020/1503 of 7 October 2020 on European <i>crowdfunding</i> service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937) Payments: Final Guidelines on Authorisations of Payment Institutions (EBA-GL-2017-09)
Enabling innovative business models to reach EU scale	ESA proportionality and flexibility in financial regulation for innovative <i>FinTech</i> business models	Innovation Hubs and <i>Sandbox</i> DLT Pilot Regime: Regulation (EU) 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU
Enabling innovative business models to reach EU scale	Regime for initial coin offerings	MICA Regulation
Enabling innovative business models to reach EU scale	Interoperability and standardization ( <i>Blockchain</i> )	Market infrastructures: DLT pilot regime
Enabling innovative business models to reach EU scale	Interoperability and standardization (application programming interfaces)	EBA industry working group on APIs under PSD II
Enabling innovative business models to reach EU scale	Enable innovative business model to scale-up across EU	Both <i>Crowdfunding</i> Regulation and MiCA enabling European passporting. DLT Pilot Regime EU wide scope. Innovation Hubs and Regulatory <i>Sandbox</i>
Supporting the uptake of technological innovation	Technology-neutrality	Expert Group on Regulatory Obstacles to Financial Innovation (ROFIED) - Thirty Recommendations on Regulation, Innovation and Finance (2019)
Supporting the uptake of technological innovation	Guidelines on outsourcing to cloud service providers, switching standards and contractual clauses	EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) DORA (restrictive for third country cloud service providers)
Supporting the uptake of technological innovation	EU Public <i>Blockchain</i> Initiative	European <i>Blockchain</i> Services Infrastructure (EBSI)
Supporting the uptake of technological innovation	Building capacity and knowledge in the EU <i>FinTech</i> Lab	EU <i>FinTech</i> Lab kick off in 2018
Enhance security and resilience	Cyber threats information sharing between financial market participants	Digital Operational Resilience Act (DORA)

<b><i>FinTech</i> Action Plan Objectives (2018)</b>	<b>Topic</b>	<b>Action taken as of 2022</b>
Enhance security and resilience	ICT security and governance requirements	Digital Operational Resilience Act (DORA)
Enhance security and resilience	Cyber resilience testing framework	Digital Operational Resilience Act (DORA)

Table 12 *FinTech* action plan overview and status as of July 2022

Source: Author

## **2. Digital Finance Strategy for the EU (2020)**

The European Commission issued the Digital Finance Strategy for the EU Communication on 24 September 2020. This strategy continues with the work performed in 2018 by assessing the key trends in digital innovation in 2020, setting up strategic objectives for digital finance, prioritising four key elements, and designing specific actions to be taken. This general strategy document is complemented specifically in the payments vertical by a secondary strategy, namely the Retail Payment Strategy) (European Commission [EC], 2020f, pp. 1-27).

The document identifies four main trends impacting the financial markets: (i) Increasing adoption of digital innovations which facilitate growing at a lower cost; (ii) Acceleration in the innovation cycles and an increasing tendency to be more open and collaborative (with specific reference to the APIs as enablers, still lacking references to DeFi products); (iii) Data and IT infrastructures as key assets; and (iv) innovation driven by new agents such as *FinTech* start-ups and *BigTechs* (Comisión Europea, 2020a, pp. 2-3).

The European Union views these trends as an opportunity. Hence, to support the strategy of embracing financial innovation, the document establishes four key priorities with relevant action plans. These priorities and action plans replicate the ones identified in 2018 and add focus on certain elements enumerated in the *FinTech* action plan, such as a clear section related to digital identities and the need to update eIDAS Regulation.

For this reason, eIDAS 2 Regulation is also subject to critical analysis in this chapter regarding those aspects which impact or are linked to the financial services industry. At the same time, the inclusion of open finance as one of the key priorities necessarily directs

the discussion towards a possible review of the existing Payment Services Directive and whether a broader regulation is needed.

The four key priorities identified, and their action plans can be seen in Table 13.

Priority	Action detail	Impacted areas
Removing fragmentation in the Digital Single Market	Enabling interoperable identities	EU -wide use of digital AML regulatory pack
	Facilitating the scaling up of digital financial services across the Single Market	Licensing requirements (for crypto related business, it is contemplated under MiCA)
Facilitate digital innovation	Enabling EU markets in crypto assets and <i>tokenised</i> financial instruments	MiCA DLT Pilot Regime Regulation MiFID II framework review
	Promoting the use of cloud computing infrastructure	EU cybersecurity agency (ENISA) Review of the NIS 1 directive (Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) Digital Operational Resilience Act (DORA)
	Promoting investments in <i>software</i> and artificial intelligence tools	Not identified
	Ensuring a future proof legislative framework on an on-going basis	Commission regular reviews and interpretative guidance
Establishing a common financial data space	Facilitating real-time digital access to all regulated financial information	Directive (EU) 2019/1024 of the European Parliament and of the Council of June 20 <sup>th</sup> , 2019 on open data and the re-use of public sector information
	Promoting innovative IT tools to facilitate reporting and supervision	<i>RegTech</i> and <i>SupTech</i> tools framework and strategy to be developed
	Open Finance	Design of <i>open finance</i> framework, need to review <i>Open Banking</i> regulation (PSD II). Alignment with EU Data Strategy, Data Governance Act proposal and Digital Services Act.
Addressing the challenges and risks associated with digital transformation	Consumer and investor protection (based on same activity, same risk, same rules)	Review of PSD II and e-Money Directive. Review of the Financial Conglomerates Directive.
	Protection of consumers and public interest	Digital Operational Resilience Act (DORA)

Table 13 Overview of priorities under the 2020 EU Digital Finance Strategy, with detail of the action plans and areas impacted.

Source: Author

Because of this analysis, three core pieces of regulatory initiatives have been produced which cover the crypto assets space (MiCA), the use of distributed ledger technologies in financial markets (DLT Pilot Regime), and the management of operational resilience in the financial sector (DORA). These three regulatory initiatives are analysed in the next sections under a common scheme: (i) objectives, (ii) main elements, (iii) observations (both general and technical), and (iv) main outcomes. Other transversal ad hoc initiatives have also been proposed as regulations for technological platforms, especially to approach *BigTech* issues in a holistic way.

Adjacent regulatory updates must also be developed for, for example, the eIDAS 2 framework, a possible PSD III, or to review anti-money laundering European regulatory frameworks. This chapter includes reflections on eIDAS 2 as well as PSD II<sup>145</sup>.

### **III. AD-HOC MODELS. MARKETS IN CRYPTO ASSETS**

#### **1. Objective**

Markets in Crypto Assets, also known as MiCA<sup>146</sup> is one of the brand-new regulatory initiatives born from the *FinTech* Action Plan of 2018 and the EU Digital Financial Strategies of 2020. As a nascent challenge the regulator has opted for a Regulation model instead of a Directive with the aim to avoid discrepant local regulations or interpretations across the region.

The regulatory objective of MiCA is to design a control framework that will drive digital innovation while maintaining an adequate balance between financial stability and customer protection. The key objectives of MiCA include reaching an equilibrium between consumer protection, financial stability, and market integrity; ensuring a level playing field among financial sector participants; and supporting high potential innovation (Comité Económico y Social Europeo, 2021, pp. 1-7).

For this reason, the regulation includes the following main elements: (i) crypto assets emission, offering, and trading; (ii) crypto-services and their providers, including

---

<sup>145</sup> The changes in the anti-money laundering regulation and specifically the travel rule requirements (information to be included in the traditional transfers as well as the crypto transactions) are used to showcase the regulatory lag theory discussed in the supervision chapter.

<sup>146</sup> Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance) PE/54/2022/REV/1.

pertinent licensing and supervision regimes; (iii) internal governance requirements for issuers, offerors, and crypto asset services providers; (iv) consumer protection; and (v) market abuse rules.

## **2. Main elements of the regulation**

The MiCA Regulation has been subject to several observations, amendments, and additions during its negotiations phase since the document was published back in 2020.

The European Council was mandated to negotiate the proposal on 24 November 2021. Trialogues between co-legislators began on 31 March 2022 (Council of the European Union, 2022) using an edited proposal that considered new elements that had increased importance in the two years lapse, such as decentralised autonomous organisations (DAOs); environmental, social, and governance components; and recent financial crime initiatives (Berger, 2022, pp. 1-159).

An agreement was finally reached on 30 June 2022 (Council of the European Union, 2022). On 10 October 2022, the European Parliament Committee of Economic and Monetary Affairs approved the final version of the regulation, which is was formally published in 9 June 2023. Some of the changes proposed in March have been modified or eliminated in this final version (e.g., several of the references to AML and the definition of DAOs in art.3.1).

The proposal's goal is to establish the legal basis for certain types of crypto assets and service providers, which are currently regulated at the European level. MiCA also aims to develop authorisation rules that would benefit innovation by developing EU passporting in the crypto space, which would be equivalent to the EU passporting rules already applicable to traditional financial players and, more recently, to crowdfunding platforms.

MiCA's content is structured into a total of nine titles. Title I focuses on the subject matter, scope and definitions. Title II addresses offerings and the marketing of crypto assets which are not asset-referenced tokens (ARTs) or e-money tokens (EMTs). Title III is exclusively focused on regulating asset-referenced tokens. Next, Titles IV and V encompass authorisations related to e-money token issuers and crypto asset services providers. Title VI establishes tools for the prevention of market abuse and uses the Market Abuse Regulation as its reference model. Titles VII and VIII establish rules



related to the public sector (supervisors). Finally, Title IX considers transitional and final provisions. The main analysis of this work is related to Titles I to VI.

### ***2.1 Subject matter, scope, and definitions***

The subject matter of the MiCA Regulation can be broadly divided into two main sections: i) requirements for the offering and placing on market of crypto assets and ii) requirements for the main actors in this industry, namely crypto asset services providers (CASPs).

As indicated in Article 1 of MiCA, the regulation includes elements such as transparency and consumer protection, authorisation and supervision regimes, governance and operational requirements, consumer protection, prevention of insider trading, control of material non-public information, and prevention of market manipulation.

With regards to MiCA's scope, it applies to “natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto assets or that provide services related to crypto assets in the Union” (MiCA art.2.1). This initial statement already contains an element for improvement in comparison with the initial proposal document as back in 202 the regulator did not seem to differentiate between crypto asset issuance and the offering of crypto assets to the public. Issuers are the person or entity that controls the creation of the crypto assets, whereas the offerors are the person or entity seeking admission to a crypto trading platform. Both roles can merge into one, but in other cases there may be different counterparties that require differentiation. This element was addressed by the European Council in its Interinstitutional File: 2020/0265 (COD) (Council of the European Union, 2021).

In terms of geographical reach, the regulation will apply to those persons or entities located in the European Union, providing services to clients in the European Union, or marketing or promoting the services in the area (Martínez, 2021, pp 41-62).

In principle, European individuals proactively requesting the services of third-country counterparties would not be subject to the regulation. However, recent discussions of the regulation have raised concerns regarding a possible circumvention of the European regulation by third-country counterparties. The draft discussed in March 2022 incorporated the following statement:

*A practice whereby a third-country firm includes general clauses in its terms of business or through the use of on-line pop-up 'I agree' boxes whereby clients agree that any transaction is executed on the exclusive initiative of the client, should not be deemed to be an attempt to circumvent this Regulation. (Recital 51; Berger, 2022, p. 16)*

This highlights a problem regarding third-country regulated services providers that have been offering services during all these years (mainly brokerage and custody). The regulation will heavily impact their cross-border business and interactions with European counterparties, potentially requiring proceeding with relevant filings in the European region to continue their activities.

A second, related open question is whether there can be a situation in which a non-European entity can issue a crypto asset-referenced in euros (euro *stablecoin*) that, in order to avoid MiCA requirements, would not be offered to European-based individuals or corporations. Again, the reality seems to surpass the theory, as Circle (a US-based global financial technology firm) announced in June 2022 the issuance of a euro-backed *stablecoin* that will not be traded in the European region nor offered to the European public (Circle, 2022, pp. 1-7). Rather, this *stablecoin* will be offered in global exchanges, used in DeFi protocols, and offered in main financial non-EU hubs such as the United Kingdom or United States. However, the EU may not benefit from this product due to its avoidance of regulatory burden (Sandner et al., 2022, pp. 1-9). Circle may decide to abide by US regulatory frameworks and supervision that align with other products offered (e.g., US-backed *stablecoins*) and to avoid supervisory fragmentation or inefficiencies.

This approach, however, may not be totally clear. Per art.48.2 of MiCA clearly indicated that, 'an e-money token which references a Union currency shall be deemed to be offered to the public in the Union'. Coordination between regulators may be required under these circumstances to evaluate how to proceed. The real case already exists; it is now the authorities' responsibility to address the challenge. In the meantime, until MiCA is fully implemented in 2024, there will be a euro-backed *stablecoin* that is neither supervised by an EU regulator nor offered to the EU public.

With regards to the delimitation of crypto assets and the types of crypto assets covered, the regulation excludes crypto assets that may be covered in other regulatory

regimes. MiCA defines a crypto asset broadly in art.3.1 (5) as a “digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology”, which includes financial and non-financial crypto assets and does not differentiate between fungible or non-fungible assets. Under this approach, known excluded cases such as algorithmic *stablecoins* or non-fungible tokens could be potentially interpreted as subject to MiCA requirements. Thus, this approach could produce unintended consequences. For example, it would potentially mean that inadequate crypto assets such as denominated privacy coins (i.e., crypto assets used for money laundering and terrorist financing purposes) would be included in the scope of the regulation and would be offered by crypto asset services providers.

However, MiCA does not establish a holistic token taxonomy to define its scope, in contrast with other crypto regulations such as the US (Congress.gov, 2021, pp. 1-14), or Andorra (Govern d’Andorra, 2022, pp. 1-76). This may have been done intentionally to avoid being too detailed and to allow MiCA to function as a future-proof regulation given the constant emergence of new types of tokens. Nonetheless, as there is no general agreement on an adequate token taxonomy, MiCA’s lack of a comprehensive token taxonomy has resulted in a confusing and partial regulation.

In this way, MiCA (art.3.1 [6], [7], and [9]) only covers fungible tokens classified as (i) asset-referenced tokens or ARTs (*stablecoins* that maintain their value by referring to the value a basket of fiat currencies, one or several commodities, one or several crypto assets, or a combination of such assets. ARTs also include the referencing to any value or right or combination of those, to be able to be future-proof); (ii) electronic money tokens (also known as e-money tokens or EMT, which are a type of *stablecoin* or a payment token that aims to maintain a stable value by referring to one single fiat currency; the last version clarifies that those e-money tokens that maintain the value of a fiat currency in the EU shall be considered electronic money under the Electronic Money Directive); and (iii) utility tokens (other crypto assets that are intended to provide digital access to a good or service, available on DLT, and only accepted by the issuer of that token).

For those crypto assets not included in this taxonomy, it could be argued that Article 3.1 (5) would apply by default in the case of fungible tokens issued by a non-identified counterparty (e.g., Bitcoin; Muñoz, 2021, p. 9). For this reason, fungible tokens cannot be subject to the issuance requirements of MiCA, but crypto asset services providers

offering services linked to these tokens can nonetheless be subject to the controls of the European regulation.

MiCA reflects a clear evolution regarding these concepts to prevent becoming outdated even before the regulation's publication. However, MiCA's definition of utility token still refers to acceptance only by the issuer and access to a good or service provided only by the issuer of the token. In principle, this definition neglects cases in which there are several issuers or the token is used by several operators, which is the current tendency in Web 3.0 projects (Jennings, 2022, pp. 2-28). As such, this definition is a subject of critique in this work because it makes the content outdated (implying a failure of the future-proof principle).

There are several observations regarding these definitions. First, both ART and EMT can fall under the category of payment tokens if used as a means of payment. Second, the definition of ART seems to be based on the assets that back the token, whereas EMT and utility tokens seem to be defined based on their use or purpose. Third, neither of these definitions seem to include cases of hybrid tokens (tokens that have several purposes or uses, e.g., as a means of payment and investment, investment and utility, or all three: payment, utility, and investment). Additionally, as mentioned, the use of tokens is dynamic: it evolves with time, and therefore a token initially designed as a payment token may be used by the public as an investment token. Moreover, the total of the structure is based on the issuance of these crypto assets by identified or identifiable counterparties, and, in principle, it would not cover instances in which there is no identifiable person issuing the crypto asset. The current framework would not work for crypto assets issued by non-identifiable persons and thus requires alternative considerations. However, the solution would not lay in the hands of a European regulator or supervisor alone but would require a minimum global consensus or a decentralised minimum rule of 'compliance by design'.

Both asset-reference tokens and e-money tokens (in sum, *stablecoins*) include specific sub-classifications of the denominated 'Significant' ART and EMT.

The specifics of the crypto asset taxonomy are a foundational element in determining the obligations for issuers and crypto asset services providers. For this reason, it undergoes specific analysis in Section 2.2.

It should be noted that other types of *stablecoins* (algorithmic *stablecoins*) were initially considered out of MiCA’s scope and are currently not specifically indicated in the body of the regulation. However, Recital 41 of MiCA establishes that Title III or IV will apply to these subcategories of *stablecoins*. The main reason for the last-minute inclusion is the negative impact of the algorithmic *stablecoin* TerraUSD crash on crypto financial markets in 2022 (Shen, 2022, p.1).

Moreover, the regulation is missing key elements from the risk-based approach perspective (especially in relation to consumer protection), such as a differentiation between wholesale *stablecoins* (non-retail client-facing crypto assets) and retail *stablecoins* (retail client-facing crypto assets). The first type can be used between institutions and agents for internal purposes (efficiency improvement in terms of clearing, settlement, and liquidity management) and would represent a lower risk from the general public.

In summary, the regulations applicable to crypto assets may vary and are not MiCA-exclusive, as can be seen in the table below.

Type	MiCA	Other specific (direct/ main)
<b>Public</b>		
Central Bank Digital Currencies (CBDC)	Excluded (Recital 13)	No
<b>Private</b>		
<i>Stablecoin</i> - asset referenced <i>token</i> (ART)	Yes	No
<i>Stablecoin</i> -significant asset referenced <i>token</i> (SART)	Yes	No
<i>Stablecoin</i> - e-money <i>token</i> (EMT) – payment <i>tokens</i> backed on a single non-EU currency	Yes	No
<i>Stablecoin</i> - significant e-money <i>token</i> (SEMT)	Yes	No
Utility <i>tokens</i>	Yes	No
Other <i>tokens</i> (payment <i>tokens</i> )	Yes (residual)	No
Crypto assets (financial instruments) - security <i>token</i> or investment <i>token</i>	No	Directive 2014/65/EU (MiFID II), Regulation (EU) No 600/2014 (MiFIR), Regulation (EU) No 596/2014 (Market Abuse Regulation), Directive 2014/57/EU (Market Abuse Directive), Regulation (EU) 2017/1129 (Prospectus) and Regulation (EU) 2022/858 (Pilot)

Type	MiCA	Other specific (direct/ main)
Crypto assets (deposits)	No	Directive 2014/49/EU (Deposit Guarantee Schemes Directive)
Crypto assets (structured deposits)	No	Directive 2014/65/EU (MiFID II), Regulation (EU) No 600/2014 (MiFIR), Regulation (EU) No 596/2014 (Market Abuse Regulation), Directive 2014/57/EU (Market Abuse Directive), Regulation (EU) 2017/1129 (Prospectus) and Regulation (EU) 2022/858 (Pilot)
Crypto assets (electronic money) – payment <i>tokens</i> backed on a single EU currency	No	Directive 2009/110/EC (Electronic Money Directive) and Directive (EU) 2015/2366 (PSD II)
Crypto assets securitization	No	Regulation (EU) 2017/2402 (Securitization Framework Regulation)
Hybrid crypto assets	No clear mention	No
Non-fungible <i>tokens</i>	Partially excluded	No

Table 14 *Overview of the existing token main European regulatory framework (excluding transversal financial regulations such as financial crime (Directive (EU) 2015/849), tax or consumer protection related)*

Source: Author

Focusing on the token types under MiCA, depending on their classification, their issuers are subject to different levels of licensing and operating requirements. Hence, it is important to review crypto asset taxonomy.

## **2.2 Crypto assets taxonomy in MiCA**

Title II (Crypto assets besides asset-referenced tokens or e-money tokens) is a sort of ‘crypto regulation by default’ in that it applies to those crypto assets that are not ARTs or EMTs and that do not fall under the categories excluded from the regulation. However, there are also implicit exclusions, such as the CBDC that are mentioned in Recital 13 of MiCA, non-fungible tokens for non-financial related purposes in Recitals 10 and 11 of MiCA, and crypto assets issued by a non-identifiable counterparty.

Regarding this, art. 4.1 (a) requires crypto assets other than AMT and EMT to be issued by a legal entity. However, due to the recent development of decentralised autonomous organizations (DAOs), the version from March 2022 included a structural change that impacted several aspects: first, this article would no longer applicable to issuing crypto assets but rather to offering them. Moreover, the offeror would no longer limited to a legal person because the current requirements under Title II would apply to a legal entity

established in the Union, a natural person having its residence in the EU, or other entity established or having seat in the EU and subject to the rights and obligations of the EU, or a decentralised autonomous organisation. However, this specification was eliminated in the final approved version of MiCA, limiting the offer to legal persons via art. 4.1 (a)

Replicating the existing Prospectus Regulation, a white paper should be generated by the crypto asset offeror (art. 4 MiCA). A white paper can be defined as the ‘technical document that must contain a minimum of information about the operation to be carried out’ (Otero, 2021, p. 191). White papers have been used extensively for several purposes, including as a marketing document (to attract investors) and as an analogy of the requirements already in place for financial instruments.

The influence of Regulation (EU) 2017/1129 on MiCA is evident. Even, in the draft shared on March 2022, the definition of qualified investor directly cited Article 2 of the Prospectus Regulation, which itself referred to the Annexes of MiFID II listing the categories of professional clients and eligible counterparties. The final version published on June 2023 directly points to the MiFID II Annex II to simplify the normative.

In the specific case of ‘crypto assets by default’ (including utility tokens), the obligation should be covered by the offeror. This point differs from ARTs or EMTs where the obligation falls with the issuer. However, as observed by Otero, the requirements under MiCA seem to be stricter and more exhaustive in comparison with the requirements of the Prospectus Regulation (Otero, 2021, p. 193).

A white paper, which should be declared to the national competent authority and published on the Internet, is not required when the tokens a) are offered for free; b) they are automatically created as a reward for the maintenance of the distributed ledger or the validation of transactions (cases of staking and mining); c) the offer concerns a utility token providing access to a good or service that exists or is in operation; d) the holder of the token has the right to use it only in exchange for goods and services in a limited network of merchants with contractual arrangements with the offeror if there is no specific direct or indirect benefit from the offerors; e) an offer to fewer than 150 natural or legal persons per Member State where such persons are acting on their own account; f) over a period of 12 months, starting with the beginning of the offer, the total consideration of an offer to the public of a crypto-asset in the Union does not exceed EUR 1 000 000, or the equivalent amount in another official currency or in crypto assets; g) an offer of a crypto-

asset addressed solely to qualified investors where the crypto-asset can only be held by such qualified investors. (art.4.2 and 4.3 MiCA).

As demonstrated, Title II predominantly focuses on transparency and consumer protection (disclosure) requirements, while the other two types of crypto assets (and their significant versions) will be subject to specific licensing, authorisation, governance, and operational requirements.

There are no authorisation requirements, but white papers and marketing materials should be notified to the competent authority 20 working days before publication (art.8.5 a MiCA).

Regarding marketing materials and communications in general (for all types of crypto assets), in the specific case of Spain, the Royal Law Decree 5/2021 introduced an amendment to art.240 bis of the Royal Law Decree 4/2015 that permits the Spanish CNMV to authorise and control crypto assets marketing and communications activities as well as to establish the criteria for the marketing of crypto assets. Electronic money institutions (and their products and services) were already covered in the Circular 4/2020 of Bank of Spain (*Circular 4/2020, de 26 de junio, del Banco de España, sobre publicidad de los productos y servicios bancarios.*). However, other crypto asset services providers were still out of scope. For this reason, the CNMV issued Circular 1/2022 in January 2022 to specifically regulate crypto assets marketing initiatives (*Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión*).

This circular is key from the European perspective as it was the first to regulate this activity among Member States with the aim to protect consumers. The Spanish initiative applies to all crypto assets under MiCA used for investment purposes, and its scope is extensive and includes not only explicit promotions but also implicit promotions, trainings, courses, and workshops. The circular not only applies to crypto asset services providers but also to influencers. The obligation entails a notification 10 days prior to launching marketing promotions, and the CNMV can request amendments or even stop initiatives.

It should be noted that the concept of crypto asset services addressed in the CNMV Circular is different from the MiCA proposal and therefore may be impacted once MiCA comes into force, although it can be argued that the last two types of services in the



Spanish circular – namely (i) any form of remuneration of crypto assets, and (ii) any other services or activities whose purpose is the commercialization of crypto assets – would be comprehensive enough to cover all MiCA services as well as non-specified services.

In any case, marketing communications will need to be characterised by three main elements: first, all advertising communications should be identified as such (identification). Second, the information provided should be impartial, clear, and not misleading (veracity). Finally, advertising materials' content should be coherent with the corresponding white paper (congruence) (Tapia, 2021a, p. 8).

Returning to crypto assets 'by default', users contracting crypto assets that fall under Title II have the right to withdraw within 14 days from the day of the consumers' agreement to purchase the assets (art.13.1 of MiCA). This right will apply when the token is obtained directly from the issuer or from a crypto asset services provider placing crypto assets on the issuer's behalf. The right also applies to any consumer who has purchased crypto assets that are subsequently the subject of a modified crypto asset white paper. It will not apply when crypto assets are admitted for trading on a trading platform for crypto assets prior to the purchase by the retail holder (art.13.4 of MiCA).

The second level of requirements (which could be considered as medium) would apply to asset-referenced tokens (ARTs), which are regulated in Title II (art.16 to 47 of MiCA). The first and most obvious difference is the requirement of a pre-authorization ahead of the tokens' issuance, which will be exempted only if (a) over a period of 12 months, calculated at the end of each calendar day, the average outstanding amount of asset-referenced tokens does not exceed EUR 5,000,000 or the equivalent amount in another currency, and the issuer is not linked to a network of other exempt issuer; or (b) the offer to the public of the asset-referenced tokens is solely addressed to qualified investors, and the asset-referenced tokens can only be held by such qualified investors (art.16.2 of MiCA).

However, a white paper for ARTs will apply in all cases as there are no exemptions. The white paper will need to be provided and approved as part of the authorisation package to be presented before the authorities. An ART's white paper is based on the same requirements for crypto assets 'by default', but it also includes several other requirements under art.19 of MiCA, such as information related to the issuer, about the token, the offer or its admission to trading, rights and obligations, underlying technology,

risk warnings, reserve of assets and any ESG related impact. Specific guidelines for white papers (mainly format) will require further development according to Regulatory Technical Standards (RTS).

Similar to the banking industry, the request to operate via a European passport is possible. The authorisation process begins from the moment that the authorisation request is considered completed. Once considered as completed, the national competent authority will issue a draft decision that will be shared with the EBA, ESMA, and ECB, which will issue an opinion within two months of receiving the draft decision from the local authority. Once obtained, the authorization can be revoked under different circumstances (art.20 MiCA).

Once authorisation is obtained, the ART issues will be subject to a set of obligations (art.27 to 35) which range from generic (e.g., to act honestly, fairly, and professionally; provide transparency and customer protection; ensure adequate governance frameworks) to specific (e.g., conflict of interest procedure, complaints handling procedure, stress testing, and own funds).

Final version also incorporated reporting obligations to ESMA under art.22, which will require further development via level 2 rules. In this way, MiCA tends to mirror requirements already in place in the financial industry (CRD V and CRRII). The chapter also includes stipulations with regards to the investment of reserve assets, prohibition of interest, and the process around potential acquisitions of ART issuers; the last of these replicates the Financial Holding Directive. Thus, it can be considered a comprehensive set of rules.

The third level of requirements would apply to e-money tokens (EMTs) under Title IV of MiCA (art. 48-58). This is a more restrictive set of rules because, instead of designing specific authorisation norms, it directly requires any EMT issuer to be authorised as a credit institution or electronic money institution (EMI). The same authorisation exemptions that have been assigned to the EMI and credit institutions will apply to the e-money token issuers.

As such, stronger access barriers as well as control frameworks have been imposed on EMTs. This may be the underlying reason why EMT white papers are considered equivalent to crypto assets 'by default' (including utility tokens) and therefore notification applies instead of pre-authorisation for the issuance of EMTs.

The authorisation is exempted in cases equivalent to ARTs, but the white paper would need to be created, notified, and published in the web of the issuer. MiCA also included a new authorisation exemption under Art 48.4 for EMTs indicating that the dispensations made under Directive 2009/110/EC of 16 September 2009 (e-money Directive) will also be extended to e-money tokens. The question here is that the art. 9 of this Directives leaves the option to the EU Member States to apply certain waivers or not, and therefore, is not consistent across the EU. Therefore, this reference could potentially bring regulatory arbitrage in the region.

The EMT title also focuses on the issuance and redeemability of EMTs, establishing that issuance should be at par versus the funds received from the public. Therefore, it can be interpreted that the reference should be 1:1, and tokens issued according to a lower ratio will not be catalogued as EMTs even though they may be partially backed and used as a means of payment. The issue then becomes that they would be neither EMTs nor ARTs because the definition includes those cases of tokens referenced to fiat currencies but not those cases of tokens referenced to a single fiat currency that are partially backed. As such, in principle, these cases would fall into the crypto assets 'by default', with a low-risk regime equivalent to utility tokens.

The EMT white paper is in principle like the ART in structure and must include clear indications that the EMT is neither covered by the investor compensation schemes, nor by the deposit guarantee schemes (art. 51 of MiCA). Regulatory Technical Standards will need to be developed to specify the different requirements of the EMT and ART white papers.

Finally, both ARTs and EMTs have an enhanced control framework for those cases in which there is an issuance of a significant ART or a significant EMT; both would usually be known as global *stablecoins*). Issuers or tokens meeting certain objective criteria will be considered under this regime, but issuers of tokens can also apply voluntarily to be considered significant *stablecoins*. In this case, issuers will be subject to EBA supervision that replicates the model and criteria of the single supervision mechanism in the banking sector.

According to art.43 MiCA two of the following points must be met for a token to qualify as significant: i) the number of holders of the asset-referenced token is larger than 10 million; ii) the value of the asset-referenced token issued, its market capitalisation or

the size of the reserve of assets of the issuer of the asset-referenced token is higher than EUR 5 000 000 000; iii) the average number and average aggregate value of transactions in that asset-referenced token per day during the relevant period, is higher than 2,5 million transactions and EUR 500 000 000 respectively; iv) the issuer of the asset-referenced token is a provider of core platform services designated as a gatekeeper in accordance with Regulation (EU) 2022/1925 of the European Parliament and of the Council; v) the significance of the activities of the issuer of the asset-referenced token on an international scale, including the use of the asset-referenced token for payments and remittances; vi) the interconnectedness of the asset-referenced token or its issuers with the financial system; vii) the fact that the same issuer issues at least one additional asset-referenced token or e-money token, and provides at least one crypto-asset service.

Entities that meet these criteria will be subject to further requirements to ensure the financial stability of crypto markets. For this purpose, a remuneration policy is needed. Moreover, enhanced controls related to liquidity, stress testing, minimum own funds, wind-down plans, and custody of tokens will apply (Arts. 45 to 48).

### ***2.3 Crypto assets service providers (CASP)***

Crypto asset service providers (CASP) are defined under art. 3.1. (15) of MiCA as any person whose occupation or business is the provision of one or more crypto assets services to third parties on a professional basis and that is allowed to provide crypto asset services.

Crypto asset services are exposed under 3.1. (16) via *numerus clausus*, indicating that these services entail: a) providing custody and administration of crypto assets on behalf of clients; b) operation of a trading platform for crypto assets; c) exchange of crypto assets for funds; d) exchange of crypto assets for other crypto assets; e) execution of orders for crypto assets on behalf of clients; f) placing of crypto assets; g) reception and transmission of orders for crypto assets on behalf of clients; h) providing advice on crypto assets; i) providing portfolio management on crypto assets; j) providing transfer services for crypto assets on behalf of clients;

Notably, Recital 79 of MiCA clearly indicates that crypto asset services should be considered ‘financial services’ per Directive 2002/65/EC requirements for distance marketing.

It should also be noted that MiCA creates two general categories of supervised entities, which are equivalent to those involved in primary markets or secondary markets (Paracampo, 2022, p. 152). The first (issuers of crypto assets) are regulated based on whether they issue crypto assets ‘by default’ (including utility tokens), asset-referenced tokens (ARTs) or e-money tokens (EMTs). The second, which are responsible for the circulation and distribution of the crypto assets issued, are regulated under Title V (Arts. 59 to 85 of MiCA).

In Title V, the European regulator aims to set up a cross-border, level playing field around crypto asset services providers to avoid fragmentation and regulatory arbitrage on topics such as transparency or organisational requirements. Once applies in 30 December 2024, these activity categories (crypto asset services) will be subject to financial regulation (reservation of activity and authorisation will apply to the activity and institutions) (Paracampo, 2022, pp. 152-154).

Entities with the capacity to provide crypto services can be classified into two large groups. The first group comprises entities that are already regulated under other traditional services and regulatory regimes and that will extend their services to crypto, or the Regulation will partially apply (art. 60 of MiCA). These entities include credit institutions under Directive 2013/36/EU, electronic money institutions under Directive 2009/110/EC, an entity exempted by Article 2 (5) points (4) to (23) of Directive 2013/36/EU, and investment firms authorised under Directive 2014/65/EU.

The March 2022 proposal included certain exemptions that would also be applicable to entities exempted by Article 2 (5) points (4) to (23) of that directive, central counterparties, authorised under regulation 648/2012/EU (central securities depositories), authorised under regulation 909/2014/EU, and regulated markets authorised under directive 2014/65/EU. These activities have now been reflected in the current art. 60 of MiCA.

In the case of Spain, the requirements applicable to electronic money institutions would potentially extend to hybrid electronic money institutions and to hybrid payment institutions as per Law 5/2015.

It is notable that in the March 2022 version, apparently, existing entities with a license to provide custody and administration services would not been considered under the exemptions in Article 2 and would therefore be potentially subject to authorisation under

Title V (art.55), as indicated by Alvarado Herrera. This could have increased the burden of counterparties, (Alvarado, 2021, pp. 249-250) due to the potential overlap of regulatory elements. This was clarified in the MiCA published version, which includes a 40 working days notification requirement for these agents.

The second group comprises crypto asset services providers (CASPs). These new agents can be divided into several sub-categories:

CASPs already operating under a national regulation and registered before a national competent authority (e.g., Spain, Germany, or France) (Paracampo, 2022, p. 156). In such circumstances, both crypto assets issuers that require authorisation and crypto asset services providers are able to continue operating on a transitory regime after MiCA's publication or until they are granted authorisation. Crypto-asset service providers that provided their services in accordance with applicable law before 30 December 2024, may continue to do so until 1 July 2026 or until they are granted or refused an authorisation (art. 143.3 of MiCA)

Newly established or non-regulated CASPs that are fully subject to the MiCA authorisation process. The full Title V will only apply to these counterparties through an ad hoc statutory rule (Paracampo, 2022, p. 156).

This differentiation was criticised by Paracampo as it could potentially generate an uneven playing field where CASPs that are already authorised and have lighter requirements would be able to operate, while other participants would still be in the process of being authorised.

The crypto asset services providers articles can be grouped into three main themes. The first relates to authorisation, its extension and withdrawal, registration, cross-border activities, and the provision of services by third-Member State entities. It could also entail regulatory approval in a potential CASPs acquisition scenario.

The second theme relates to transparency, integrity, and customer protection, which include general principles such as acting honestly, fairly, and professionally; prudential requirements; the safekeeping of clients' crypto assets and funds; a complaint handling procedure; and the prevention, identification, management, and disclosure of conflicts of interest.

The third theme relates to organisational and governance requirements (management body, organisational structure, fit and proper requirements, financial-

crime-related internal requirements, internal control mechanisms, risk assessments, business continuity plans, market abuse, know-your-customer policies, and outsourcing controls, among others).

Specific stipulations are included depending on different activities as ad hoc requirements in Chapter III of Title V (arts.75- 82 of MiCA). These activities include (i) custody and administration of crypto assets on behalf of third parties, (ii) operation of a trading platform for crypto assets, (iii) crypto exchange, (iv) execution of orders for crypto assets on behalf of third parties, (v) placing of crypto assets, (vi) reception and transmission of orders on behalf of third parties, and (vii) advice.

### ***2.3 Market abuse***

Market abuse is treated as a transversal topic under Title VI (Arts. 86 to 92). The articles tend to replicate at a high level the requirements contemplated in the investment services industry (mainly via MiFID II, the Market Abuse Directive, and the Market Abuse Regulation) to create a simplified version that is nonetheless comprehensive enough to cover crypto assets. The requisites mainly focus on insider dealing governance stipulations (prohibition and prohibition of unlawful disclosure) as well as market manipulation banning. These articles seem to reflect the several cases in which it has been evidence a weak control framework of the CASP on this topic, even under a broader concept which would be conflicts of interest management.

Currently, there are several types of market abuse that impact the crypto industry at the global level, such as pump and dump (United States District Court Southern District of New York, 2022), wash trading (Cong et al., 2021, pp. 1-50)<sup>147</sup>, frontrunning<sup>148</sup>, and insider trading (United States District Court Western District of Washington Seattle Division, 2022)<sup>149</sup>.

To achieve adequate customer protection and financial stability, these practices should be eliminated, and the CASP should use controls to mitigate these risks and prevent them from causing uncertainty in the sector. Therefore, this initiative to extend market abuse requirements to issuers, offerors, and CASPs are welcomed.

---

<sup>147</sup> Manipulation technique wherein an entity creates artificial trading volume by executing trades against itself.

<sup>148</sup> The entity benefits from accessing market information before the public because of its role or privileged position, obtaining a non-ethical benefit from it based on information asymmetry and market information.

<sup>149</sup> The use of material non-public information (MNPI) or insider information for own or personal benefit via trading strategies.

This may be one of the weakest points of CASPs as the focus has thus far been on financial crime. CASPs have followed this stream to maintain in the European market and seek means of collaboration with traditional financial players. However, other compliance-related topics will require further development in the crypto industry to provide adequate assurance and protection to the general public and the new crypto financial system.

### **3. Observations**

#### ***3.1 General critics and aspects for improvement***

The first question to address is whether MiCA achieves its purpose of designing a common framework for the European Union ‘to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose’ (von der Leyen, 2019, p. 6). MiCA is a comprehensive initiative that covers much of the crypto space and its risks. MiCA’s objective not only concerns controls but also the promotion of innovation. It is precisely this point that may not have been totally considered, for example, in Article 140.2 (z) indicating that the Commission will present a report to the European Parliament and the Council on the application of MiCA to perform ‘an appraisal of whether any changes are needed to the measures set out in this Regulation to ensure consumer protection, market integrity and financial stability’. However, this paragraph does not refer to supporting or evaluating the impact on innovation and competitiveness in the region.

Moreover, the crypto asset space has been developed largely by small and medium-sized enterprises, many of which are start-ups that operate based on financing rounds. These funds are obtained via venture capital and business angels, which are used to seeing customer early traction metrics (short-term results) to decide on their next investment. However, under MiCA, a good portion of these funds would be invested into capital requirements, governance, and internal controls, which may sometimes be too burdensome for these types of entities. Hence, MiCA seems to be stricter than existing financial regulations in several aspects, such as certain elements of the authorisation process and exemptions, the MiCA white paper is based on the Prospectus Regulation (Regulation [EU] 2017/1129).

Art.3.2 (b) of the Prospectus Regulation specifies an exemption when ‘the total consideration of each such offer in the Union is less than a monetary amount calculated



over a period of 12 months which shall not exceed EUR 8,000,000'. However, all the MiCA token limits are below EUR 5,000,000 (Zetsche et al., 2020, p. 25-26).

The second question is whether MiCA qualifies as a future-proof regulation. The final 2023 version includes several key elements that were absent in its initial publication on 24 September 2020, including activities captured under crypto asset service provision. In less than two years, general elements such as environmental clauses had to be added.

Despite these additions, there are still several key areas of development, such as DeFi or financial related smart contracts that have not been addressed. CBDCs and EMT are another example given that entities offering distribution services of CBDC or EMT as well as crypto asset services may be subject to the MiCA limitations (Zetsche et al., 2020, p. 25-26) or fragmentations (subject to one regime for crypto assets and to a different future regime for public crypto assets).

Additional example of omitted topics is new ways of investing such as crypto staking, earning, or farming as well as other types of crypto services such as crypto-loans (including flash loans), crypto-insurance, or retirement investments in crypto assets (currently covered in the US proposal regulation S.4356 Lummis-Gillibrand Responsible Financial Innovation Act of 6 July 2022). Finally, there are elements which have been addressed only superficially, such as the previously mentioned DAOs or forks.

Regarding forks, depending on the level at which they are produced, they can result in a myriad of consequences with important legal implications. A potential hard fork on the basis layer can have ramifications for all the services and businesses running based on it due to the composability and interdependencies that have been created. Bitcoin blockchain experienced a hard fork (resulting in Bitcoin and Bitcoin Cash), but in this case Bitcoin is limited to transactions. It does not include services based on smart contracts such as those created by Ethereum and the subsequent Blockchains. A hard fork in these structures can potentially impact all dependent services.

In these cases, questions such as whether the assets should be moved to the consensus Blockchain without customer consent or what kind of notification should be made remain open, particularly in cases of contentious forks. Furthermore, whether there is any sort of obligation from the CASP to provide information, analysis regarding the fork, and whether this type of information constitutes advice for clients remain unsolved. Elements such as security, market capitalisation, community support, trademark, and services

migrated to the forked Blockchain need to be evaluated (Guillaume & Riva, 2022, p. 44-47).

Similarly, MiCA does not clarify requirements, implications, or transparency obligations for forks that impact the general operations of service providers. There can even be scenarios in which a fork of the issuer of a significant *stablecoin* would generate two legal entities, causing the underlying assets to split. Clients and volumes could then be impacted to the point that the significant *stablecoin* would disqualify as such.

From the operational perspective, this reality requires service providers to create operational and control procedures for operating under these circumstances and approaching clients.

Additionally, MiCA is heavily influenced by MiFID II. This causes confusion as to which types of crypto assets would be considered under MiCA and which would qualify as financial instruments under MiFID II. We agree with the critiques of Alonso Ledesma, Muñoz Pérez, and Ibañez Jimenez regarding the issues that MiCA creates. As indicated by these authors, the lines are blurred because of several circumstances, such as the dynamic characteristics of the crypto assets; the possibility of having hybrid or mixed categories (falling under both MiCA and MiFID II); and the fact that the crypto asset definition in MiCA is broad and could cover financial instruments, but the rules to identify tokens falling into unclear categories have not been described (Alonso, 2021, p. 69-77; Ibañez, 2021, pp. 25-39; Pérez, 2021, pp. 117-135).

Following on from this, MiCA does not solve how to proceed in the case of hybrid tokens or tokens that evolve to have a new purpose, both of which have been common issues in the crypto space in recent years.

As such, MiCA may not be future-proof and could require a review or amendments within a few years after its implementation. Furthermore, additional regulations will be required to cover certain elements such as NFTs (non-fungible tokens), along with a general overarching token taxonomy regulation that would go beyond the tokens already included in MiCA.

The third and final general observation relates to how MiCA interacts or correlates with other regulations. MiCA appears to replicate several requirements listed in MiFID II, causing doubt regarding whether crypto assets are considered a semi-investment

product even in cases in which they are used as a means of payment. This results in stricter controls (related to the authorisation process or white papers) with attractive benefits (e.g., [i] generating interests as related to that part, they would be treated as a means of payment equivalent to the electronic money directive and PSD II; [ii] exemption limits of EUR 5,000,000 instead of EUR 8,000,000). Therefore, the same activity, same risk, and same rules are not achieved in this regulatory piece. Moreover, certain cases carry an extra burden for new activities, including possible regulatory overlaps. Therefore, the principles of proportionality or a risk-based approach are not achieved either.

### ***3.2 Technical questions and observations***

Technical observations regarding MiCA relate to the (a) elements addressed in the regulation, such as the significant ART and EMT criteria or the liability regime; and (b) omitted elements such as the lack of distinction of the type of DLT, the lack of specifications in relation to smart money (also known as programmable money), source code use, or the interaction between traditional financial service providers and crypto-service providers.

Elements addressed in the regulation:

The first point worth mentioning is the liability regime. The initial 2020<sup>150</sup> version of MiCA's art.67.8 made the providers of custody and administration services responsible for any event, including external ones. This wording would have meant a strict liability regime for crypto-custody and administration services, which would have classified this activity as high risk or heavily regulated in comparison with traditional finance requirements (e.g., UCITS depositaries). As a result, this activity would become unattractive in the EU space (Zetsche et al., 2020, p. 20).

The March 2022 draft already addressed this issue as follows:

*(...) Crypto asset service providers that are authorised for the custody and administration of crypto assets on behalf of third parties shall not restrict the liability to their clients for the loss of crypto assets or of the means of access to the crypto assets as a result from an operational incident associate with the provision of the service or the operation of the service provider or including*

---

<sup>150</sup> 'Crypto-asset service providers that are authorised for the custody and administration of crypto-assets on behalf of third parties shall be liable to their clients for loss of crypto-assets as a resulting from a malfunction or hacks up to the market value of the crypto-assets lost' (Art. 67.8 of MiCA).

*malfunction or hacks that are attributed to the provision of the relevant service and the operation of the service provider. The liability of the crypto asset service provider shall be up to the market value of the crypto asset lost. (art.67.8 MiCA, March 2022 draft)*

The final art. 75.8 of MiCA Regulation indicates:

*Crypto-asset service providers providing custody and administration of crypto-assets on behalf of clients shall be liable to their clients for the loss of any crypto-assets or of the means of access to the crypto-assets as a result of an incident that is attributable to them. The liability of the crypto-asset service provider shall be capped at the market value of the crypto-asset that was lost, at the time the loss occurred.*

*Incidents not attributable to the crypto-asset service provider include any event in respect of which the crypto-asset service provider demonstrates that it occurred independently of the provision of the relevant service, or independently of the operations of the crypto-asset service provider, such as a problem inherent in the operation of the distributed ledger that the crypto-asset service provider does not control.*

Nevertheless, it is unclear how the market value of the crypto asset lost should be calculated, necessitating clarification of this point. Moreover, the question lies on who is responsible and to whom should the consumers claim in cases of problems on the DLT or the coding of the tokens, specifically for those classified as decentralized. In this way, there is a consumer protection gap in the substance of the activity itself, which may not be totally understood by the consumers.

Elements not contemplated in the proposal:

The technical elements not included in the proposal relate to the technological side of MiCA. As mentioned, MiCA tends to mirror what is already familiar to the European regulator. As such, it is split between payments regulation (Electronic Money Directive and PSD II) and investment regulation (MiFID II, MAD, and MAR). However, the key element underlying crypto is sometimes missing as it relates to technology, not to finance.

Key concepts such as the distinction between types of DLT (e.g., private, and public) and the roles and responsibilities of relevant counterparties related to financial services are clearly missing. On the same note, the use of smart contracts for financial purposes is not included, even if these contracts can potentially raise programmable money that would operate automatically based on given conditions. Finally, the code source, which is the basis for digital assets, is also omitted. These two notions (smart contract and code source) have been regulated in order draft initiatives such as the American one, which defines smart contracts as

*(...) computer code deployed to a distributed ledger technology network that executes an instruction based on the occurrence or non-occurrence of specified conditions; or any similar analogue; and includes taking possession or control of a digital asset and transferring the asset or issuing executable instructions for these actions.* (Congress.gov, 2022)

This definition is used in the US proposal and requires the redemption of *stablecoin* funds to be based solely on a smart contract; issuers should state that they comply with this requirement. Smart contracts are also discussed in the decentralised finance sections, which refer to the need to ensure the accuracy of the information used in the smart contract.

With respect to the source code definition in the American document, the text states that it ‘means the source code version comprising a digital asset; and does not include *software* used to manage or facilitate transactions in a digital asset’ (Congress.gov, 2022).

Source code is used in relation to customer protection requirements (pre-notification of the material source code version changes in digital assets). It is also related to contractual arrangements.

*(...) at the initiation of a contractual relationship, agree in writing regarding the source code version the person will use for each digital asset and the treatment of each asset under the law, including securities and commodities laws and the Uniform Commercial Code applicable to the transaction SEC. 502. SOURCE CODE VERSION OF DIGITAL ASSETS.* (Congress.gov, 2022)

The requirements around source code extend to possible changes or modifications to the source code (different validation rules), the need to evaluate changes to the source code version from an impact assessment point of view, and the requirements to maintain specific standards.

Hence, there are key innovation elements impacting the financial space that, due to their technological characteristics, have not been contemplated in the MiCA Regulation. Furthermore, key crypto-exclusive agents seem to be missing, such as Oracles or the cross-chain service providers which enable interoperability between the outside world and the *Blockchain* or between different *Blockchains*.

Given the above points, MiCA lacks crypto-specific counterparties that must be addressed.

#### **4. Main outcomes: MiCA II before even publishing MiCA I**

MiCA is a key initiative of the Digital Finance Strategy and the *FinTech* Action Plan. It has become a strategic component of the future European financial system. It is also a comprehensive initial step that addresses the need to set common standards across the region by avoiding fragmentations at an early stage.

However, between 2020 and 2022, the draft underwent amendments regarding financial crime, ESG, and operational resilience. Moreover, new concepts were addressed, such as DAOs, forks, and activities like crypto portfolio management. The final Regulation published in June 2023, partially eliminated some of these elements.

Importantly, MiCA may jeopardise innovation in the European space by imposing heavy regulatory burdens on the main focus of the crypto industry, namely small and medium-sized enterprises.

There is an important inconsistency between the controls implemented in MiCA per crypto asset type and risk. If we take the example of EMT and ART regimes and disclosures, EMTs (tokens backed 1:1 versus a fiat currency) will be subject to the requirements imposed by electronic money institutions and payment services. Moreover, a white paper will need to be produced for this type of *stablecoin*. A crypto asset issued may only be partially backed by a currency (for example, 60%-backed crypto asset); under this condition, the volatility and risk may be higher. We consider this scenario as an equivalent to a derivative under MiFID II. However, in principle

these cases may qualify as asset-reference token per MiCA's current description of these as 'a type of crypto asset that is not an electronic money token and that purports to maintain a stable value by referring to the any other value or right or combination thereof, including one or several official currencies of a country'. Thus, a partially backed crypto asset under the ART issuance requirements may be subject to lighter rules though the underlying risk is higher than EMTs, unless it is clarified in further Regulatory Technical Standards that these situations fall under MiFID II scope.

Moreover, derivatives under MiFID II are considered complex products (European Securities and Markets Authority [ESMA], 2014, pp. 2-3) and are therefore subject to enhanced disclosure, suitability, and appropriateness requirements that are absent in the MiCA framework, causing a mismatch between the underlying risk and controls for that risk.

Regarding the issuance of *stablecoins*, the probability of a majority of *stablecoins* being deemed significant is potentially high, and the risk of *BigTechs* as crypto asset services providers would be underestimated.

Specific crypto agents, such as Oracles, as well as interoperability service providers are missing. Likewise, services such as loans, flash loans, insurance, staking, and farming are not addressed, and technological terms (source code and forks) have been ignored. Interactions between regulated entities and DeFi space are increasing, and even central banks have started experimenting with DeFi interactions; however, there are no current guidelines around this space, which impedes the progress under stable rules of the game (Bank of International Settlement, 2022, pp. 1-3).

MiCA cannot be categorized as fully proportional nor future-proof and will therefore require review soon after it has been published.

#### **IV. AD-HOC MODEL OF DLT PILOT REGIME**

The DLT Pilot Regime Regulation (Pilot) (Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65) is the second of the three main regulatory pieces framed within the EU Digital Finance Strategy published on 24 September 2020. The DLT Pilot Regime Regulation can be defined as the basic rule for setting up an ad

hoc regulatory sandbox in the European Union for trading, clearing, and settling tokenised securities and token securities.

The following sub-sections describe and evaluate (i) the objective of the proposal, (ii) its main advantages, (ii) observations regarding operations under the DLT structure (transacting and settlement) and technical observations, and (iii) main outcomes.

## **1. Objective**

The Regulation shows that the European regulator has realized that the idea of one size fits all does not work in this new innovative environment, and therefore, has applied a new perspective by which the authorized participants will present what could be defined as a business model proposal or business plan approach (Zetzsche & Woxholth, 2021, pp. 18-20). Conscious of the fact that the existing regulatory structures for markets - mainly MiFID II, MiFIR and the CSDR (Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 in improving securities settlement in the European Union and on central securities depositories and amending Directives 98/23/EC and Regulation (EU) N° 236/2012) – the regulation displays a range of exemptions that the participants can request.

As deduced from the previous comments, the norm aims to support innovation by reducing the existing regulatory barriers in the European Union. This includes exemptions to MIFID II, MiFIR and CSDR<sup>151</sup>.

In this way, it also endeavours to provide legal certainty in terms of regulation and supervision linked to technological innovations in the markets infrastructures (Barrio, 2021). This legal certainty would include consumer and investor protection as well as financial stability (Dentons, 2020, p. 35).

Finally, Pilot has been designed with the idea to allow experimentation both from private and public side in an adequate and controlled environment where the supervisor can better grasp the potential and risks of the DLT applied to this vertical, and obtain

---

<sup>151</sup> Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 Text with EEA relevance.



a more comprehensive understanding on its impact on the existing regulations (Annunziata, p. 305).

However, due to the limitations that will be described in the next section, it should be highlighted that these objectives would only be attained partially, for existing participants and possibly under non-attractive or efficient circumstances due to the limitations of the model and the fact that there are already initiatives in production environment operating and testing similar concepts (e.g., bond issuance via DLT structures).

## **2. Main elements**

The first element to be considered is the fact that the regulatory scope is limited according to the art. 2 of Pilot to multilateral trading facilities operating in DLT systems (DLT MTF), settlement systems operating in DLT systems (DLT SS), and the trading and settlement systems operating within DLT systems (DLT TSS). This combination of TSS (Art 2.10 Pilot)<sup>152</sup> would not be allowed to be performed by the same entity under the traditional markets infrastructure scope.

The DLT MFT refers to a multilateral trading facility that only admits to trading DLT financial instruments (Art 2.6 Pilot). In its initial draft version, the figure was further described as able to be operated by ‘an investment firm or a market operator, that only admits to trading DLT transferable securities and that may be permitted, on the basis of transparent, non-discretionary, uniform rules and procedures, to: (a) ensure the initial recording of DLT transferable securities; (b) settle transactions in DLT transferable securities against payment; and (c) provide safekeeping services in relation to DLT transferable securities, or where applicable, to related payments and collateral, provided using the DLT MTF’ (art.2.5 Pilot draft). Accordingly, the DLT MFT can also settle transactions. In these cases, they are termed DLT TSSs, and the same entity can trade and settle.

The DLT SS are operated by a central securities depository (CSD) that settles transactions in DLT transferable securities against payment. To quote the text, ‘a settlement system that settles transactions in DLT financial instruments against payment or against delivery, irrespective of whether that settlement system has been designated

---

<sup>152</sup> “DLT trading and settlement system” or “DLT TSS” means a DLT MTF or DLT SS that combines services performed by a DLT MTF and a DLT SS’ (Art. 2.10 Pilot).

and notified in accordance with Directive 98/26/EC, and that allows the initial recording of DLT financial instruments or allows the provision of safekeeping services in relation to DLT financial instruments' (art.2.7 Pilot). Thus, the regulation focuses on trading on venue and omits bilateral trading (i.e., systematic internalizers and over-the-counter deals).

The scope also reflects that the regulator is focusing on already established entities with the required licenses per the relevant regulations (MiFID for DLT MTF, CSDR<sup>153</sup> for DLT SS, and both for DLT TSS). This leaves out DeFi solutions for which there is no legally regulated entity and smart contract (the code) is the law. Hence, access to the *sandbox* is in practice restricted to established regulated financial entities.

Crypto trading platforms, offering crypto qualifying as securities, would in principle fall under the definition of DLT MTF and therefore require authorisation using MiFID II rules, which would not be applicable to solutions based on decentralised autonomous organisations (Navarro, 2021, pp. 65-98). There are also questions regarding the central securities depository role as this agent would be less attractive than the DLT TSS, which can trade and settle. Moreover, if an open distributed ledger technology is used, the role of the central securities depository may be redundant. Therefore, it is probable that the regulator had a private permissioned *Blockchain* in mind when designing this regulation, although it is not totally clear (Barrio, 2021, p. 128). By using this type of *Blockchain*, the central securities depository would still hold a centralised role. Permissionless or public DLT are not mentioned, and thus this regulation is not 100% technologically neutral as it would only cover a DLT subcategory. In reality, there have already been cases of digital bonds issued on public *Blockchain*, as is the case of the European Investment Bank (EIB, 2021, p.1).

Another omitted element would be operations via bulletin boards<sup>154</sup> (a sort of semi-secondary market), which is a structure that crypto assets platforms have been using that is a grey area separate from multilateral trading facilities or organised trading

---

<sup>153</sup> REGULATION (EU) No 909/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (Text with EEA relevance).

<sup>154</sup> "A bulletin board exclusively advertises trading interests without facilitating in any way the interaction of those interests, unlike a trading venue. It might include prices, quantities available, and even display the contact details of potential buyers and sellers, however it cannot organise the bringing together of these interests, nor use a centralised order book or any other kind of trading system." (European Securities and Markets Authority [ESMA], 2021, p. 27)

facilities (OTF). This concept has not been clarified in MiFID II but is raised in one of the MiFID II review reports (European Securities and Markets Authority [ESMA], 2021, pp. 27-30). The bulletin board displays bid and offer interests but does not match the orders and therefore is not considered in the MTF or OTF of MiFID II.

Regarding products that are within the scope of the *sandbox* regime, it is limited to shares and certain types of bonds. In the case of the shares, the actual or tentative market capitalisation of the issuer of DLT transferable securities should not reach EUR 500 million (initial proposal was 200 million). In the case of convertible bonds, covered bonds, corporate bonds, other public bonds, and other bonds, the issuance size should be less than EUR 1 billion (initial proposal was 500 million) (Art 3.1 Pilot). There are two options for how those would be represented: (i) financial instruments issued in the traditional way (off-chain) that are afterwards represented in the *Blockchain* (tokenised financial instruments or tokenised securities) or (ii) financial instruments directly issued on-chain and, therefore, token securities.

If we compare the MiFID II financial instruments' scope *versus* Pilot, we can conclude that the money markets instruments, derivatives, and units in collective investment undertakings were initially out of scope from the product perspective in the first drafts of the regulation (Navarro, 2021, p. 86). However, the final published Pilot Regulation has included in scope units in collective investment undertakings covered by Article 25(4), point (a)(iv), of Directive 2014/65/EU, the market value of the assets under management of which is less than EUR 500 million.

In terms of product range, the operational limits described in Arts.3.2 and 3.3 of Pilot indicate that

*The aggregate market value of all the DLT financial instruments that are admitted to trading on a DLT market infrastructure or that are recorded on a DLT market infrastructure shall not exceed EUR 6 billion at the moment of admission to trading, or initial recording, of a new DLT financial instrument.*

*Where the admission to trading or initial recording of a new DLT financial instrument would result in the aggregate market value referred to in the first subparagraph reaching EUR 6 billion, the DLT market infrastructure shall not admit that DLT financial instrument to trading or record it.*

*Where the aggregate market value of all the DLT financial instruments that are admitted to trading on a DLT market infrastructure or that are recorded on a DLT market infrastructure has reached EUR 9 billion, the operator of the DLT market infrastructure shall activate the transition strategy and shall notify the competent authority of the activation of its transition strategy and of the timescale for the transition (...).*

This scope appears limited to illiquid types of bonds and will therefore reduce the activity cases that fall into secondary markets (International Capital Markets Association [ICMA], 2022, p. 5); this would also mean that in most operations, the asset acquired would be maintained in the books of the financial entity, with a lower possibility of considering further steps to obtain liquidity from the crypto asset.

For both types of business, the entities wishing to operate need to provide a detailed business plan specifying components such as resources, technological and operational infrastructure, and legal arrangements that would grant legal certainty to the markets (e.g., liabilities, governing law, pre-litigation dispute settlement mechanism, or the applicable jurisdiction in case of legal action; art.7 Pilot). In this way, the operator entity identifies the applicable jurisdiction and therefore the home state supervisor which will manage the request for exceptional handling and compensatory measures. This request is submitted to the home country authority, which will evaluate and interact with the applicant. Permission should be previously shared with ESMA. ESMA will provide a non-binding opinion to grant adequate consistency and proportionality across the European Union. This report should be issued within 30 days from its submission (Arts. 8.7 and 9.7 Pilot).

Once approved, ESMA will publish the lists of participants, start and end dates, and permissions and exemptions on its website as a transparency exercise. This indicates that although the request and decision is in the hands of national authorities, there is a strong desire to maintain coordination or centralisation within the European Securities Markets Authority.

In both cases (DLT MTF and DLT SS) the relevant regulations apply (MiFID II and MiFIR for DLT MTF, and CSDR in the case of DLT SS and TSS). However, the operators can request a close list of exemptions established at the European level to be granted via special authorisation from the national supervisor, which would include

certain conditions or compensatory measures (Arts. 4 and 5 Pilot). This is a tricky element given that for a DLT TSS, the operator would have to request exceptional handling from both the regulator in charge of banking and the regulator in charge of securities, thereby adding complexity to the process.

The DLT MTF includes the possibility to trade securities recorded on the DLT MTF's distributed ledger rather than in a central securities depository (if requested by an operator of a DLT MTF, the competent authority may permit that operator to admit natural and legal persons to deal on own account as members or participants) (art.4.2 Pilot), thus preventing the DLT MTS from requiring a DLT SS. Another important exemption for the central securities depository and for those entities operating under a DLT TSS scheme is exemption from complying with the book entry rules and certain definitions established in Regulation (EU) 909/2014 that do not fit or are incompatible with the DLT's nature. Because of this, existing regulations are not compatible with the DLT solutions and thus are not technologically neutral at this stage. To progress while the regulations adapt (countries such as Luxembourg or France have already taken measures), the proposed solution is to operate via *ad hoc* exemptions that are granted for a total of six years. Un Spain the current amended *Ley del Mercado de Valores* it would be possible to operate without the need to present the request within the DLT Pilot regime.

The author agrees with the position of Navarro Ruiz, who considers distributed ledger technology to be an evolutionary means of representing financial instruments, which were originally represented in paper, afterwards in book-entry and with this new technology, another variety of support or representation is created (Navarro Ruiz, 2019, p. 86).

EU regulation in general would need to recognise this new type of support as an alternative to the traditional book-entry solution, requiring relevant modifications in the corporate law for those cases relating to shares issuance and trading.

Regarding operations once entities have been approved to the *sandbox*, the Pilot Regime Regulation proposal establishes controls and reports. One control relates to the general limit of EUR 9 billion. If EUR 9 billion is reached, a transition strategy is triggered (art.3 Pilot). This transition strategy should have been previously proposed by the operator, approved by the authority, and made public to the participants (art.7 Pilot), and it will include a time plan.

The questions that arise are what the expectations of the authorities are: do they expect the operators to partially reduce the volumes to go below the risk thresholds established, or would this trigger a total migration? In either case, the key element is that the activity would need to be migrated back to the legacy systems used by the MTF or SSS. An alternative option would be to continue within the Pilot regime but increase the control requirements proportionally or, for consolidated models, to evaluate the possibility of operating in an open environment. None of these scenarios seem to have been visualised by the regulator because this is just a temporary (long-term) regime, but the question of what happens afterwards remains, as indicated in Art 10.2 of the initial draft of Pilot:

(...) the Commission may propose any appropriate modifications to the Union framework on financial services legislation or harmonisation of national laws that would facilitate the use of distributed ledger technology in the financial sector as well as any measures needed to bridge the transition of DLT market infrastructures out of the pilot regime.

What is clear is that the EU is conscious of the need to evolve and move forward with adapted regulations, as indicated in Recital 53 of Pilot “If the pilot regime is successful, it could be made permanent by amending relevant Union financial services legislation to establish a single coherent framework.” Therefore, we can expect changes in this regard in the next 6 years.

### **3. Advantages**

One of the main benefits of Pilot is that it allows operation within the European area under the same terms agreed with the national authority (business plan, contingency measures, and exemptions). The so-called EU Passport valid for up to 6 years is reflected in Arts. 8.11 and 9.11 of Pilot.

The use of these new technologies may increase the speed of operations and produce more cost-efficient results that would consequently reduce fees for clients. Increased disintermediation and the capability of the DLT TSS to trade and settle would reduce time and the costs of intermediaries.

This disintermediation extends throughout the supply chain as Pilot allows to apply for an exemption from MiFID II rules demanding operations via intermediaries (trading

venues). Hence, crypto assets platforms can engage via direct interaction with the public, thereby preventing the need for investment services entities, banks, or other authorised persons to intervene and reducing costs for the public. This will also quicken the process and eliminate possible time-to-market delays that counterparties might generate (in this case, third-party dependency to reach the end user or investor). Even in an optimal scenario trading with a DLT TSS, no other intermediaries would be required (see below).

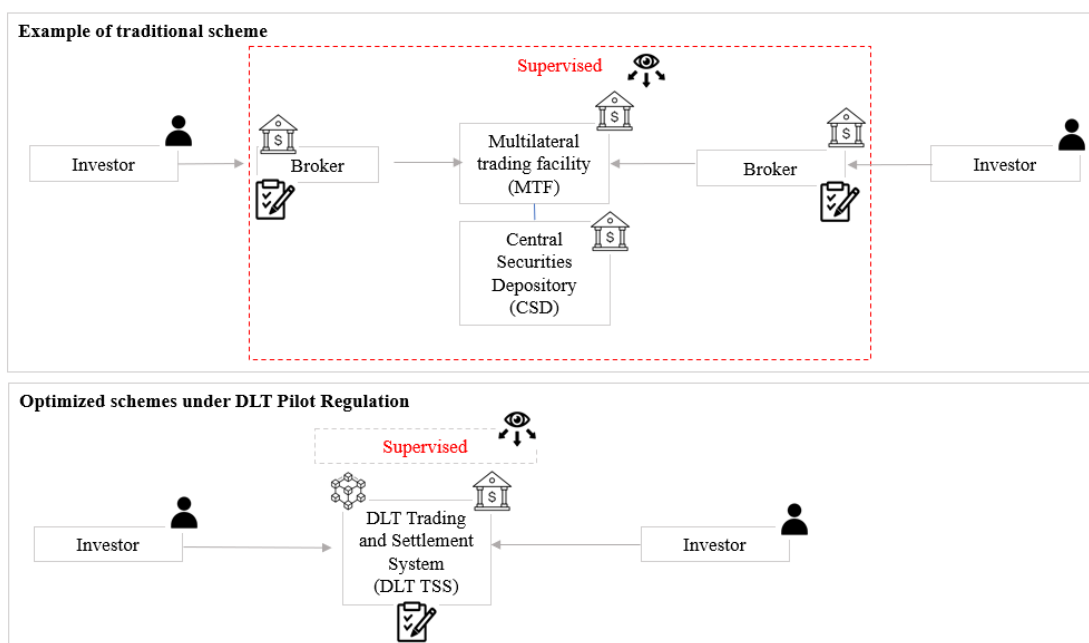


Figure 56 Comparative of traditional Operational scheme versus optimized scheme under DLT Pilot Regulation

Source: Author

Per Figure above, under the DLT pilot model, investors would not require trusted third parties such as brokers and could instead deal directly with a DLT trading and settlement system (TSS). The minimum structure requires no multilateral trading facility or central securities depository as most tasks would be automated or performed via atomic settlement within seconds.

Moreover, the distributed ledger technology would potentially allow the authorities to directly access the data required for certain reports (via node), which would not need to be reconciled in each participant layer. However, this benefit has some caveats. The information sourced may be partial (e.g., in cases of securities issued in two tranches, one off-chain [traded and settled in the traditional way] and the other on-chain).

Financial crime checks and monitoring could also be enhanced by sharing verified digital identities or users in smart contracts; this would allow direct checks against sanctions lists and maintenance of identified non-risk users in whitelists.

#### **4. Observations**

##### ***4.1 Operations and Settlement via distributed ledger technology***

The regulatory proposal is a temporary regime that will allow business models based on distributed ledger technology to evolve in the European Union despite differences between Member States in the treatment of *token* securities. In this way, authorities will be able to grasp how these models operate and can implement any necessary regulatory changes without interrupting innovation.

However, the scope of the proposal is limited, and it may be unattractive for investment. Therefore, it runs the risk of being considered a secondary option by big *incumbents*, reducing the interest and therefore efforts on this space. At the same time, *FinTechs* would be able to access collaborations with traditional finance players, but it is improbable that they would access by themselves due to licensing barriers.

Additionally, the regulation does not capture the composability or ‘Lego’ concept. As Article 2 (11), for example, indicates, DLT-transferrable securities are issued, recorded, transferred, and stored using a DLT, as if all steps should take place in the DLT, which is not necessarily true. Hence, *tokenized* securities issued off-chain and afterwards represented on-chain can potentially be considered out of scope. This definition also highlights a discrepancy with the proposed art.3 (1) (5) of MiCA that only refers to the possibility of being “transferred and stored”, not requiring to be issued in the DLT (Zetsche & Woxholth, 2021, p. 26). Whether tokenized assets have been intentionally left out of scope is an open question, but a full open option (including both native securities and tokenized securities) would have been a better option for participants to experiment within the sandbox. Even hybrid options would be attractive but are out of scope.

In relation to the settlement element, there are discussions of when the transaction will be considered settled in the *Blockchain*. In principle, this would be dissociated from the moment that the transaction is executed, which occurs once the parties agree (off-chain or on-chain) with the terms and conditions. Settlement takes place once the parties



are discharged of their obligations and the operation is irrevocable. This step has two components: 1) securities and 2) cash transfer according to CSDR. However, if the DLT pilot regime is complemented with other experimental projects related to cash legs such as CBDC, the settlement would take place within seconds.

If the transaction is agreed on-chain, the time between the agreement and the settlement will be almost immediate, with settlement defined as (i) the moment in which the required majority of the nodes have validated the transaction or (ii) when the block has been added to the chain. In the case of private permissioned *Blockchains*, this type of transaction would be accomplished within seconds. In any case, when the transaction is considered irrevocable will depend on the legal terms and conditions of the agreements.

Concerning cash transmission, CSDR requires the settlement to be executed with central bank money, with commercial bank money as a secondary option. Both cases would introduce barriers in DLT-based operations because the delivery of securities would need to take place simultaneously. For this reason, Pilot allows exemptions and enables participants to settle via e-money tokens (art.5.8 Pilot). However, this regulation does not refer to the use of central bank digital currencies, which represent a strong future use case.

To return to the ‘Lego’ concept in DLT market infrastructures, there can be hybrid solutions that mix off-chain and on-chain solutions until technology and the markets mature. It would also potentially address different types of chains with non-identical rules. For this reason, Pilot must consider supporting interoperability between the traditional finance environment and the DLT pilot space, as well as different chains (Association for Financial Markets in Europe, 2022, p. 3-4).

#### ***4.2 Technical***

From a technical perspective, there are three main elements: (i) the use of a regulation instead of directive (policy technical strategy), (ii) the potential use of permissioned *Blockchains*, and (iii) impact on regulatory technical standards (RTS). The technical strategy used (regulation instead of directive) reflects the regulator’s aim to avoid discrepancies among Member States and to promote standardisation of the rules that should apply in this sandbox. It also sets up *numerus clausus* regarding the

exemptions that can be applied,<sup>155</sup> limiting the manoeuvrability of national authorities. It is unclear whether national authorities will be able to ask for ‘an exceptional handling of the exceptional handling’ for new scenarios requiring more flexibility. Zetzsche and Woxholth noted that Pilot does not make specific references regarding clearing and recording requirements; thus, these may be elements that require consideration from the local authorities (Zetzsche & Woxholth, 2021, p. 14).

Concerning the second technical aspect, as described the regulation focuses on a specific sub-set of distributed ledgers (Barrio, 2021, p. 128). This is evidenced in the language used in initial draft Recital 28 (‘proprietary DLT’) and Recital 49, which allowed responsibility to participants for flaws in the underlying technology of the DLT market infrastructure. Recital 39 and art.7.2 also mention that

*(...) Operators of DLT market infrastructures shall establish or document, as appropriate, rules on the functioning of the distributed ledger technology they use, including rules on accessing the distributed ledger, on the participation of the validating nodes, on addressing potential conflicts of interests, and on risk management including any mitigation measures to ensure investor protection, market integrity and financial stability.*

Hence, the regulator does not focus on open (permissionless) DLT, which would restrict cases that have already happened in practice.

Regarding the third element (impact on regulatory technical standards or RTS), there are several concepts and fields that do not quite match the legacy requirements, including the concepts of ‘cancellation’ and ‘amendment’, which in the DLT world would not have sense once the operation has been settled on the distributed ledger. The only way to reverse these transactions would be via a contrary operation that would be considered separate, not a cancellation (Association for Financial Markets in Europe, 2022, pp. 20-21).

Similarly, ISIN numbers would need to flag or record those financial instruments issued, traded, or settled using distributed ledger technology. There are also questions around how to treat cases in which financial instruments are partially issued in the

---

<sup>155</sup> Article 4 addresses exemptions for DLT multilateral trading facilities, Art. 5 contains the exemptions for central securities depositories operating as a DLT settlement system, and Art. 6 lists exemptions for investment firms and market operators operating as DLT transaction and settlement systems.

traditional way and partially DLT-based. Moreover, ISIN numbers are the basis of several regulatory reports that would need to consider new solutions or amendments (Association for Financial Markets in Europe, 2022, pp. 20-23).

There are also questions surrounding several reporting fields required by MiFIR, where the field to be reported is the euro only, blocking the use of e-money *tokens*. Reporting related RTS will also need to be reviewed. Thus, it is expected that RTS 1 to 3 (transparency) and RTS 22 to 25 (reporting and registry) may be subject to changes in the future (Finreg 360, 2022, p.1-2).

## **5. Main outcomes**

The Pilot regime embraces an innovative mindset from the regulatory perspective: it allows entities to propose a business plan and to request temporary exemptions for those cases in which innovation would be restricted or non-compliant with European regulations. From a *FinTech* point of view, the Pilot initiative may not be attractive because entities would have to first complete a license approval process, which is usually lengthy and resource intensive. Therefore, small start-ups may be discouraged from participating.

From an *incumbent* point of view, the Pilot initiative may be less attractive than initially thought for the abovementioned reasons: there is a limitation from the product perspective, and there is no clear picture of what will happen afterwards, while investment in the setup of these models may be high. The uncertainty combined with these limitations may leave this sandbox as a secondary option for established regulated entities. Big financial entities have already launched initiatives in the production environment, and it would be easier for them to set up projects in jurisdictions such as Switzerland or Luxembourg that already manage and allow the issuance of DLT-based financial instruments.

In conclusion, the regulation may need to clarify and remove restrictions such as authorised participants, products, type of DLT, limits, and transition periods to be attractive for all counterparties.

## **V. AD-HOC MODEL OF OPERATIONAL RESILIENCE IN EUROPE: DORA**

### **1. Objective**

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and to amend Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance) (also known as DORA) is one of the main components of the European digital finance package in the 2018 *FinTech* Action Plan (European Commission, 2018, pp. 1-18). New technologies bring new risks, and one of the main focus areas in recent years has been operational resilience, including cybersecurity. This regulatory need was detected downstream as well as upstream, with the European Supervisory Authorities (2019) raising concerns in a joint technical advice document issued in 2019.

Additionally, the COVID-19 crisis has accelerated the use of digital solutions at the global level. In the words of Satya Nadella, CEO of Microsoft, ‘We saw two years of innovation in two months – with resilience, agility and flexibility being key for financial institutions to address these unique external circumstances’ (Microsoft, 2021).

As a consequence of the 2008 financial crisis, the resilience topic had already been approached from a financial perspective in terms of credit risk, capital, liquidity, and solvency requirements. However, the so-called ICT risks (Information and Communication Technologies risks) had not been adequately addressed while the dependency of the financial sector on new technologies has been increasingly growing during the last years (European Commission, 2020e, pp. 1-2).

The aftermath of this has been patch up articles disseminated along different regulations or technical standards, together with local jurisdictions developing their own solutions in an uncoordinated fashion, causing overlaps, duplication, and frequent cross border barriers for global financial actors.

Moreover, new financial agents such as the *crowdfunding* platforms or crypto assets service providers were not captured under the regulation in general, and the increasing dependency of the traditional financial institutions on technological services providers

together with data services providers, had not been properly managed in a standardized way.

In the meantime, the increase in cybersecurity threats – estimated as costing the EU financial sector between EUR 2 and 27 billion per year (Wuermeling, 2021, p. 3) – prompted the European Union to develop a general strategy for data in 2020 based on four main elements: fundamental rights, data protection, safety, and cybersecurity measures (European Commission, 2020e). The answer to this request has been the review of the Directive on Security of Networks and Information Systems (also known as NIS 1), which is a horizontal directive with requirements not only for the financial sector but also for other sectors such as energy.

For this reason, DORA aims to reach a consistency in the European area in terms of financial regulations (avoiding gaps, overlaps or different approaches) as well as alignment with bigger strategies such as NIS 2 Directive<sup>156</sup>.

## 2. Main elements

DORA's design is based on seven elements: (i) scope of the regulation, (ii) governance, (iii) ICT risk management measures, (iv) incident reporting, (v) digital operational resilience testing, (vi) third-party risk, and (vii) information sharing.

(i) One of the main novelties of this proposal is the scope of entities subject to it and identified as 'financial entities' according to Article 2. This concept (financial entities) may be misleading as the regulation includes classical agents as well as recently onboarded agents (*crowdfunding* platforms, crypto asset services providers, issuers of crypto assets, issuers of asset-referenced tokens, and issuers of significant *stablecoins*). There are also entities and activities that do not belong to the financial supervisor's realm, such as data reporting service providers, statutory auditors and audit firms, administrators of critical benchmarks, and ICT third-party service providers (art.2.1 DORA).

Furthermore, a wide range of services fall under the scope of ICT third-party service providers. According to the initial draft of art.3 (15) of DORA, this concept included 'an undertaking providing digital and data services, including providers of cloud computing

---

<sup>156</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)

services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services'. The final definition is even broader and includes hardware, cross-referencing ICT services which include

(...) digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services. (art.3 [21] of DORA draft)

Final approved concept of DORA is more generic, but still broad in relation to ICT services definition as it “means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services”.

The only exemption specified is the case of microenterprises, which is beyond the scope of this regulation to avoid excessive regulatory burden.

The personal scope encompasses numerous heterogeneous participants, with different activities and underlying realities. However, these substantial differences are not reflected in the regulatory piece. Moreover, it is unclear whether a financial regulator can extend the scope of supervision to a mixed population on a topic that is not financially related, and which could instead be seen as related to technological or general operational risk.

(ii) In terms of the second element (governance), Article 5 of DORA explicitly assigns the management body of these ‘financial entities’ the responsibility to define, approve, and oversee the ICT risk management framework along with accountability for the adequate implementation of this framework in organisations. This includes, among other things, setting the risk appetite, developing ICT business continuity policy and ICT disaster recovery plans, and approving and reviewing ICT audit plans. This article, like the majority of those discussed in Chapter II (ICT risk management), may be too detailed for a level 1 rule, leaving the entities subject to this regulation with limited power to take a risk-based approach.

(iii) The second part of Chapter II (Articles 6 to 16) includes a detailed description of the ICT risk management requirements with regard to different technical standards. The framework includes strategies, policies, procedures, protocols, and tools (art.6.8 of DORA), and it clearly establishes the requirement to maintain the three lines of defence model for ICT functions, implying that all entities subject to this requirement must establish a first level (information technology), a second control level (common second-line-of-defence functions are compliance or risk management), and a third line for independent control function (i.e., internal audit). Only microenterprises would be outside of these requirements.

This model is not a regulatory requirement for many of the entities covered by the new regulation and therefore would imply a restructuring or reorganization for them. External auditors, a merger, or second line and third-line-of-defence functions in medium-sized corporations often follow a proportionality principle. However, this is not included in the current draft and would necessitate extra resources for ‘financial entities’.

Articles 8 to 14 include the typical control life cycle of identification, prevention, detection, response and recovery, backup, staff knowledge, communication, and awareness enhancement.

The final published version of the DORA Regulation includes art.15, which leaves further harmonisation needs to the supervisory authorities. The EU Supervisory Authorities set standards via the Joint Committee and in consultation with the European Union Agency on Cybersecurity (ENISA) to ensure coordination with other European initiatives, such as NIS 2.

Finally, art.16 considers the possibility of a simplified risk management framework for certain low-risk cases or entities that are already regulated to avoid overburden, applying a risk-based approach and adequate proportionality.

(iv) The fourth pillar of the DORA Regulation pivots around ICT incident reporting (Chapter III, Arts. 17 to 23 of DORA), which include the monitoring, log, and classification of ICT-related incidents as well as the process of reporting to competent authorities via standardised templates. The requirements include initial, intermediate, and final reports to the competent authorities. This is not something new; there are already reporting requirements in place under different regulations, such as the data protection regulation (in case personal data has been compromised) or PSD II (payment-related

data). The novelty in this case is Article 21, which delineates the possibility of further centralisation of major incident reporting in a single hub. Article 23 confirms that operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions should be covered by the regulation, causing possible overlaps with existing banking requirements.

(v) The fifth element relates to digital operational resilience testing requirements. Chapter IV (Arts. 24 to 27 of the DORA) has been heavily criticised by the private sector because it imposes periodic tests to be performed by the subject entities. The initial draft was also heavily criticised because it did not apply the proportionality principle. Some of the initial draft articles imposed a detailed resilience testing program, such as the following:

(...) the execution of a full range of appropriate tests, including vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing, or penetration testing. (art.22.1 of DORA draft)

The final published version corrected this issue by linking the requirements of art.25 (testing ICT tools and systems) with art.4 (2), which refers to ‘(...) proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations (...)’. Additionally, the list of tests to be performed is not mandatory as the word ‘shall’ is included before them.<sup>157</sup> Testers must be certified. If internal resources are used as testers, previous approval from the competent authority is needed. The authority will evaluate whether the financial entity allocates enough full-time resources and ensure that there are no conflicts of interest in the tests’ design and execution.

(vi) The penultimate topic addresses ICT third-party risk (Arts. 28 to 44). Similar to the digital operational resilience testing requirements case, the third-party risk chapter (Chapter V) kicks off with a specification of the general principles, which include the requirement to follow the proportionality postulate concerning the scale, complexity, and

---

<sup>157</sup> “(..) vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing” (Art. 25.1 DORA).



importance of ICT-related dependencies as well as the risk arising from contractual clauses (art.28.1 [b] of DORA). However, like the previous case, the articles following these general principles are highly detailed and could be seen as more adequate for level 2 regulation (regulatory technical standards) rather than level 1 regulation. For example, the chapter includes specifics on the elements to be considered before entering contractual arrangements, contract execution, follow-up during the business relationship, and termination and post-contractual interactions.

Article 30 establishes models for key contractual provision, including nine general requirements and six further specific requirements for critical outsourcing that need to be included in agreements covered by the regulation. If any of those are not materially accomplished during the business relationship, the financial entity would consider this a contractual breach and would therefore terminate the relationship per art.28.7 (a) of DORA.

Section II of this DORA chapter includes the oversight framework to be established on the public side for the control of critical ICT third-party service providers, including the definition of those and the creation of a lead overseer in charge of assessing whether the critical ICT third-party service provider has adequate controls in place.

(vii) Finally, the information sharing pillar refers to the need to raise awareness of new risks originating from ICT usage and information exchange related to cybersecurity among ‘financial entities’. This chapter (Chapter VI) specifies financial entities’ obligation to notify to the competent authorities of their participation in information sharing forums or agreements. In addition, public authorities can be involved in these information sharing agreements.

### **3. Advantages**

The regulation seeks to strengthen ICT risk management rules for financial sector corporations and extends its requirements to new types of counterparties that are both financial (crypto or crowdfunding) and non-financial (e.g., auditors and technological corporations).

The basis of the regulation aims to standardise these controls across the European Area, avoiding overlapping or absent regulatory synchronisation among local jurisdictions as well as loopholes that would leave certain key cyber risk exposures

unmapped due to fragmentations in financial value chains (e.g., outsourcing of services to technological providers). The regulation also seeks to standardise diverse reporting formats to help ‘financial entities’ easily identify, and report critical or major incidents related to ICT risks.

DORA clearly indicates its status of *lex specialis* to Directive (EU) 2022/2555<sup>158</sup> (NIS 2 Directive. As mentioned in the framework of the proposal/ initiative section,

*(...) Consequently, this Regulation constitutes lex specialis with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive. (Recital 16 DORA)*

This hierarchy allows to reduce uncertainty and avoid a new potential regulatory overlap.

## **4. Observations**

### **4.1 General**

Following on from the previous point regarding *lex specialis versus* NIS, DORA does not clarify how it interacts with existing supervisory frameworks with well-developed regulations and guidelines, such as those created under the PSD II framework, including the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), and the EBA Guidelines on major incident reporting under PSD II (EBA/GL/2017/10). Moreover, there are certain terms in the existing proposal that cause discrepancies with the requirements in place.

In addition, the coherency of DORA’s principles with the core articles of the draft must be evaluated. We differentiate between principles that are present and principles that are missing.

---

<sup>158</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

In the present principles category, we identify the principle of proportionality, which can be identified in the subjective scope by excluding the microenterprises, and across the ICT risk management articles, testing related with resilience and the reporting of major incidents. Additionally, the public oversight of third-party service providers would be limited to those considered critical.

Interlinked with the proportionality principle is the risk-based approach principle, reflected in art.4 (explicit proportionality principle to be applied to Chapter II to V), art.7 (ICT systems, protocols, and tools), art.28 (principles for sound management of ICT third-party risk). The final inclusion of art.4 has allowed consideration of proportionality in the overall regulatory piece.

However, there are several elements that still go beyond a proportionality or risk-based approach. For example, by requiring a three lines of defence model or not differentiating between applicable measures based on levels of activity (for example, auditors or data analytics service providers).

The non-existent or missing main principle is the one that has been constantly mentioned when discussing innovation in finance ‘same activity, same risk, same rules’ (Lautenschläger, 2017, pp. 1-3; Hoyler, 2022, pp. 1-2; European Banking Federation [EBF], 2022a, pp. 1-24; Wuermeling, 2022, pp. 1-7). This principle is not explicitly indicated in the regulation. Moreover, if we evaluate the entities listed under the personal scope (art.2), we can identify both financial-services-related entities (including crypto assets services providers and issuers) and non-financial-services-related entities, whose activities differ widely (auditors, cloud service providers, *software*, and data centres, among others). Most of these non-financial corporations offer services across industries or to non-financial industries. Consequently, it is unclear whether these activities are covered by DORA or if there would be a fragmentation that would require non-financial entities to ring-fence their financial business or interactions with financial-related entities.

Due to the wide spectrum of underlying activities within DORA’s scope, the first element of this principle is not applied. As such, the proposed draft is inadequate because it applies the same rules to different activities that pose different risks.

Moreover, the theme of the regulation is ICT risk, which is defined in art.3 (5) as

*(...) any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.*

This definition does not make any reference to financial services as ICT risk is purely technological, which raises the question of whether financial supervisory authorities are entitled to regulate these risks or are extending their regulatory and supervisory perimeters beyond their mandates to cover risks that belong to other authorities (in this case ENISA).

In a parallel example, data protection is not regulated in the financial realm, but there is an *ad hoc* regulation in place (GDPR) as well as a standalone authority (European Data Protection Supervisor). Therefore, financial regulators and supervisors may be exceeding their mandate in several aspects: (i) activity: technology, not financial; (ii) personal scope: non-financial entities; (iii) governance: the regulation not only sets the targets for the entities, it also dictates how to reach those targets, including the setup of governance roles; and (iv) territorial scope: limitations on third-country service providers (in practice, the regulation would prohibit services offered by third-country service providers with no presence in the EU).

The question is whether financial regulators and supervisors are entitled to impose such regulations given that DORA's scope is different from the powers given to the ECB in its supervisory manual. As such, it would require a local authorisation process in several European Member States (Deutsche Börse Group, 2021, p. 10).

## **4.2 Technical**

Per the defined seven-pillar structure, we explain our technical critical observations explained below.

### **4.2.1 Scope of the Regulation and Definitions**

As indicated, the personal scope of DORA can be considered one of the main points of discussion for several reasons. First, there are entities that, although considered financial entities with similar activities and therefore similar risks, have not been included in the scope of the regulation. One example of this is consumer credit and mortgage credit

providers, as well as intermediaries which are part of the financial sector and regulated under Directive 2008/48/EC of the European Parliament and of the council of 23 April 2008 on credit agreements for consumers and Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property (EBF, 2021, pp. 6-7). Furthermore, card payment networks can have consequences on financial stability and are usually subject to cyberattacks, but they are not included in the scope of DORA.

With respect to non-financial entities, in the example of auditing entities, in principle those would be subject to the same requirements as financial entities, causing a potential overlap with their own regulations and standards, such as the International Quality Standards Management standards issued by the International Audit and Assurance Standards Board (IAASB) that already establishes governance requirements, business continuity policies, and ICT incident reporting obligations. Moreover, the European Supervisory Authorities are not their lead supervisor and therefore would not have the capacity to oversee or enforce these standards. Additionally, it is unclear how to define the supervisory perimeter as auditing firms offer their services across industries beyond finance (Accountancy Europe, 2020, pp. 1-4).

Regarding ICT third-party service providers, a financial assets group may fall under DORA's ICT third-party service provider definition and could even be classified as critical, thereby falling under double requirements that are infeasible (EPIF, 2021, p. 4).

In terms of exemptions, DORA is more restrictive than the EBA Guidelines on Outsourcing, which allows exemptions 'for market information service providers, global network infrastructures, clear and settlements between clearing houses, central counterparties and settlement institutions and their members, global financial messaging infrastructures subject to oversight by the authorities and correspondent banking services' (EPIF, 2021, p. 4). Similarly, outsourcing between entities of the same group do receive any kind of simplified regime even though they are already subject to financial regulation, resulting in unnecessary regulatory overburden for these groups.

For activity exemptions, DORA does not differentiate between frequent or continuous outsourcing and cases of *ad hoc* or one-off contracting of ICT services, which would increase the number of controls for temporary cases. This would increase costs

without necessarily improving ICT risk management, resulting in excessive overburdening for due diligence or contractual agreements for off-the-shelf software services (EBF, 2021, pp. 5-6). This approach differs from others seen in PSD II, CRR, and the MiFID II framework (Delegated Regulation (EU) 2017/565 of April 25<sup>th</sup>, 2016<sup>159</sup>). Art.30.2 (b) of the latter document excludes the purchase of standardised services, including market information services and the provision of price feeds.

The Regulation in its art. 3(60) exempts microenterprises from these regulatory obligations, but the criteria of EU Recommendation 2003/361 of May 6<sup>th</sup>, 2003, concerning the definition of micro, small, and medium-sized enterprises define a microenterprise ‘as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million’ (art.2.3). This definition does not work for small banks as the minimum balances and staff do not fall below these figures. For this reason, CRR 2 (Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013) adopted the ‘term small and non-complex institution’:

‘Small and non-complex institution’ means an institution that meets all the following conditions:

- (a) it is not a large institution.
- (b) the total value of its assets on an individual basis or, where applicable, on a consolidated basis in accordance with this Regulation and Directive 2013/36/EU is on average equal to or less than the threshold of EUR 5 billion over the four-year period immediately preceding the current annual reporting period; Member States may lower that threshold.
- (c) it is not subject to any obligations, or is subject to simplified obligations, in relation to recovery and resolution planning in accordance with Article 4 of Directive 2014/59/EU.
- (d) its trading book business is classified as small within the meaning of Article 94(1).
- (e) the total value of its derivative positions held with trading intent does not exceed 2 % of its total on- and off-balance-sheet assets and the total value

---

<sup>159</sup> Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

of its overall derivative positions does not exceed 5 %, both calculated in accordance with Article 273a (3);

- (f) more than 75 % of both the institution's consolidated total assets and liabilities, excluding in both cases the intragroup exposures, relate to activities with counterparties located in the European Economic Area.
- (g) the institution does not use internal models to meet the prudential requirements in accordance with this Regulation except for subsidiaries using internal models developed at the group level, provided that the group is subject to the disclosure requirements laid down in Article 433a or 433c on a consolidated basis.
- (h) the institution has not communicated to the competent authority an objection to being classified as a small and non-complex institution.
- (i) the competent authority has not decided that the institution is not to be considered a small and non-complex institution on the basis of an analysis of its size, interconnectedness, complexity or risk profile. (art.4 [145])

This rationale omits more entities from this regulation, considering the real business and activities with regards to the financial institutions at least.

Finally, the definitions section is not consistent with existing frameworks. For example, operational resilience does not follow the guidelines established by the Basel Committee for Banking Supervision, and several definitions are inconsistent with the FSB Cyber Lexicon. The ICT third party service provider has a different approach in comparison with EBA. (Betaalvereniging Nederland, 2021, p. 3-4).

#### 4.2.2 Governance

Turning to the governance framework, Article 5 (3) requires financial entities to have a role in monitoring arrangements and ICT third-party service providers. This entity (as a role in senior management) will oversee ICT risk exposure. It is not clear whether this role is equivalent to the Outsourcing Officer function specified in the EBA Outsourcing guidelines for entities in which there is an overlap between DORA and PSD II (EPIF, 2021, pp. 1-2).

Moreover, under DORA, the role of the management body and its responsibilities towards ICT risks are expanded in comparison with the EBA Guidelines under PSD II,

without clear guidance regarding whether a Board of Directors can delegate some of these functions to an executive board, senior manager, or a special committee.

#### 4.2.3 ICT risk management measures

This chapter of DORA has been criticised for its lack of proportionality and prescriptiveness, which will result in a soon-to-be-outdated regulation. Its lack of proportionality and risk-based approach, controls, or processes (EBF, 2021, p. 8).

Certain requirements seem infeasible. For example, Arts. 11 and 12 require a backup system in an operating environment in addition to the main system. It is unclear whether this includes having a second service provider or whether the same provider in a different location, country, or region would suffice (Deutsche Börse Group, 2021, p. 7-8).

There are also differences in terminology that can be misleading or that may lead to duplications. For example, DORA requires an ICT Business Continuity Policy and ICT response and recovery plans (art. 33 of DORA), while EBA mandates a Business Continuity Management Process (EPIF, 2021, pp. 1-2).

#### 4.2.4 Incident reporting

As previously mentioned, this proposal seems to overlap in its art 16 with the EBA Incident Reporting guidelines (European Banking Authority [EBA], 2017C, pp. 1-56) and its revised version of 2021 (European Banking Authority [EBA], 2021b, pp. 1-2). The revised version of 2021 precisely looks for a way to simplify the reporting of major incidents under PSD II, as well as the reporting templates. It also modifies the scope of security incidents and reduces the number of operational incidents that have to be reported, as a consequence of the high amount of non-substantially risk reports received by the supervisor since the implementation of the reporting requirements under PSD II (European Banking Authority (EBA), 2021, pp. 5-9). Any change of these EBA guidelines implies operational changes, once again on the operational side, with regulatory associated costs.

Again, the lack of a clear relationship between DORA, GDPR, and PSD II can lead to increased complexity for incident reporting requirements. For example, if there were a payment-related incident for a major ICT client, an entity would be required to report under DORA and possibly also GDPR. For non-ICT related incidents but major



operation incidents, PSD II and possibly GDPR requirements would apply, but DORA would not. Further exacerbating the complexity, the reporting deadlines and incident classification criteria differ among these three regulatory frameworks (EPIF, 2021, pp. 3-4).

The insufficient risk-based approach in DORA becomes apparent when comparing it with the EBA Guidelines. One example is art.10 (9) in the initial draft version, which required financial entities to report to the authorities all costs and losses caused by ICT disruptions and incidents, whereas the PSD II limits this requirement to major incidents due to the amount of work these calculations require (EPIF, 2021, pp. 3-4). This specific requirement has been modified in the final published version (current Art 11.10 of DORA), which states that the information to be provided upon authorities' request is an estimation of aggregated annual costs and losses caused by major ICT-related incidents; this approach is more aligned with the EBA Guidelines and could therefore be seen as a duplication. Moreover, the Financial Stability Board (FSB) already has a Cyber Incident Response and Recovery toolkit that provides global guidelines for incident reporting under its Effective Practices for Cyber Incident Response and Recovery report (FSB, 2020, pp. 4-18), including details on how to proceed before, during, and after an incident.

In addition, art.22 of DORA refers to feedback from the national supervisory authorities on the ICT incidents reported, but it is not clear whether that feedback would be seen as enforcements or instructions in practice, more taking into account that this is not their expertise area and there may be lack of adequate resources to be able to cope with the feedback and follow up obligations imposed to the authorities on this specific aspect (Ceyskens, 2021, pp. 5-6).

#### 4.2.5 Digital operational resilience testing

Chapter IV suffers due to the omission of a risk-based approach, by setting up a list of tests that financial entities should take. This strategy would be too prescriptive for smaller corporations and for certain types of businesses, and the details may become outdated due to new technological developments (Ceyskens, 2021, pp. 5-6).

In addition, requirements such as conducting threat-led penetration testing on live production (TLPT) for systems that support critical functions risk impacting operations for regulated services. Furthermore, there are references to developing technical standards

even though there are already technical standards in place for these types of tests, such as TIBER-EU. The possibility of each financial entity performing TLPT on their service provider, which in several cases may be the same for a part of the industry, is time-consuming and expensive. To address this, self-certification would need to be included in the current draft.

#### 4.2.6 Third party risk

Third-party risk is one of the main concerns of the private sector (Deutsche Börse Group, 2021, pp. 7-8) as there is increased dependency among financial institutions on specialised technological third-party service providers that have the capacity to offer better tested solutions with adequate standards. However, DORA would cause a regulatory barrier for three reasons: (i) imposing extreme restrictive termination requirements; (ii) imposing conditions on outsourcing or sub-contracting to third countries, thus limiting the capacity to use service providers located in non-EU countries, including developed market solutions provided from the UK, Switzerland, or the US; and (iii) demanding model contractual clauses and service agreements that may not fit or that may cause overburdening due to the numerous service types that would fall under this requirement.

Regarding the first point, art.25 (8) of the initial draft of the proposal stated that ‘financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under’ certain circumstances. Termination should be the last measure to be implemented as there may be circumstances to consider, such as the need for a timeline or the lack of other suitable service providers. The final published version includes ‘may be terminated’, thus providing more flexibility and freedom to the financial entities.

This would also apply to the scenario of the national financial regulator requiring the financial entity to suspend or discontinue use of an ICT service provider. The initial draft of art.37 (3) did not give the option to notify, remediate, and use termination as a last resort. This issue has been solved in the current art.42, which allows for this process.

In any case, these types of terminations are not immediate as the financial entity may need to find a replacement service provider, reorganise operations, and possibly notify its clients of operational changes or service interruptions due to maintenance changes or migrations. In other words, termination of critical services usually implies a

termination plan that can take weeks or months depending on the complexity and volumes. Therefore, it would need to be used as the last option or resource, and the regulation must have a flexible timeline for this type of measure.

Regarding the second point, according to art.35 (1) (d) (iv), all financial entities should refrain from ‘entering into a further subcontracting arrangement, where the following cumulative conditions are met: (i) envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country; (ii) the subcontracting concerns a critical or important function of the financial entity and (iii) the Lead Overseer deems that the use of such subcontracting poses a clear and serious risk to the financial stability of the Union or to financial entities, including to the ability of financial entities to comply with supervisory requirements’.<sup>160</sup>

This clause was initially problematic as it is now common to use third-country service providers as well as external providers, but group wise in the case of international entities. Moreover, existing cloud service providers (mainly located in third countries) would not be allowed to subcontract, which is a common practice to comply with standard service level agreements that usually require 24/7 availability (Deutsche Börse Group, 2021, p. 7-8). Therefore, DORA would prevent critical service providers in the financial industry, such as cloud services corporations, from complying with existing contractual arrangements (‘follow the sun’ or full-time availability), driving them to breach contractual agreements with the financial sector.

The limited access to these third-country service providers or sub-contractors could jeopardise access to better technologies or cost-efficient services, increasing costs for covered European entities (regulated and non-regulated) and limiting their competitive advantages (Ceyssens, 2021, pp. 5-6). UK operations for large financial groups would also be caught by this restriction.

Additionally, smaller service providers that do not fall under the microenterprise category and that operate from a third country would be banned from the EU sector due to the regulatory compliance costs to set up EU establishments (EBF, 2021, p. 29). This is also the case for third-party service providers under PSD II (initiation and aggregation)

---

<sup>160</sup> The third and last condition was not in the initial proposal draft.

or *RegTech* providers (e.g., tools related to compliance, such as transaction monitoring and filtering tools or data analytics tools).

Moreover, it is unclear what a third-country ICT service provider is. The current definition in art.3. (24) is as follows: ‘an ICT third-party service provider that is a legal person established in a third country and that has entered into a contractual arrangement with a financial entity for the provision of ICT services’. This does not clarify if a solution similar to the GDPR solution (a representative in the European Union) would suffice to avoid qualifying as a third-country ICT service provider (London Stock Exchange Group (LSEG), 2021, p. 6).

Regardless, to avoid a competitive disadvantage, the final published version of the regulation includes a third condition to limit the scope of the restriction to cases of financial stability risk or the inability to comply with supervisory requirements. Another alternative option would have been to replace the restriction with an approval or notification process (EBF, 2021, p. 34).

Finally, standard contractual clauses would need to be clearly defined as voluntary and would apply depending on the situation, which would have to be assessed by the financial entities. Renegotiation of these clauses may take time and may limit the range of possible outsourcing suppliers. Moreover, these types of contractual arrangements are usually composed of an umbrella agreement and secondary annexes that are incorporated into the evolution of the business relationship (especially those related to services and service-level agreements). Hence, clauses like those listed in the key contractual provisions article, which requires a ‘a clear and complete description of all functions and services to be provided by the ICT third-party service provider, indicating whether sub-contracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting’, may not be feasible and may require frequent amendments.

There are other minor comments to be made on this chapter, such as the fact that new regulatory reporting is required under DORA (art.28 [3]) that does not have a precedent in the EBA Guidelines, such as the annual report on the number of new arrangements on the use of ICT services, categories of ICT third party service providers, type of contractual arrangements and the services and functions provided. Another example of increased regulatory burden would be the register of information.

#### 4.2.7 Information sharing

Information sharing raises two main concerns. The first is that information sharing can include personal or highly sensitive data. As such, legal support for this data processing and sharing must be clarified (e.g., whether public interest can be claimed for these cases) (EPIF, 2021, p. 6). Due to the sensitivity of this data, there may be cases in which making it public may trigger operational risks or cyberattacks. Hence, this point should be addressed carefully.

The second source of concern is the fact that the supervisor can be part of these arrangements and requires entities to report when they are part of an information sharing group or arrangement. In practice, this makes participation almost mandatory and therefore could impact the quality of entities' interaction and participation (e.g., due to concerns about being criticised by the supervisors based on the information shared in these groups).

### **5. Main outcomes**

There are several key conclusions regarding DORA. First, as a level 1 regulation DORA needs to be flexible and reach a balance between innovation risks and controls. The current draft may be too detailed and includes elements that would be more appropriate for a level 2 regulation, resulting in overly prescriptive rules that prohibit adequate proportionality and a risk-based approach. This could result in the European financial sector becoming unattractive or too burdensome to certain service providers, who may take the strategic decision not to provide services to European financial entities. Moreover, it focuses on technological risks and issues that may be beyond financial regulator expertise; this is evidenced by restrictions and burdensome requirements that may not be viable or that may put the financial sector at risk (i.e., prohibitions on outsourcing to third countries).

Though the regulation focuses on technological issues, it may ignore exposure directly linked to related financial services and the use of technology, such as the use of foreign-state-controlled financial applications by certain sensitive populations in Europe. These types of risks are addressed in other foreign jurisdictions' regulatory initiatives, such as the American Lummis-Gillibrand Responsible Financial Innovation Act (Congress.gov, 2022). Section 603 of this proposal includes the requirement to analyse the use of the

official digital currency of the People's Republic of China on government or public official devices.

It is not clear how DORA interacts with the PSD II requirements already in place. This situation may become even more complex once the level 2 regulatory measures begin to be discussed. One option would be that PSD II and its regulatory developments would be maintained as *lex specialis* to DORA or that references to PSD II are made in level 2 regulatory standards.

Finally, the most fundamental question regarding DORA relates to its own foundations: are financial regulators entitled or qualified to regulate ICT risk, or should this be left to cybersecurity authorities? The current draft may jeopardise innovation in the EU sector, and there are several sections that are not feasible from the operational or business points of view. Hence, we question if the financial regulator is overstepping a non-financial subject.

## **VI. AD-HOC TRANSVERSAL MODELS: DIGITAL MARKETS ACT (DMA) AND DIGITAL SERVICES ACT (DSA)**

Europe currently has two regulatory proposals for establishing adequate controls on digital platforms. These are Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on fair and equitable markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Regulation or DMA) and Regulation (EU) 2022/2065 of the European Parliament and of the Council of 14 September 2022 on fair and equitable markets in the Digital Markets Regulation or DMA) and Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a digital single market for services and amending Directive 2000/31/EC (Digital Services Regulation or DSA).

In both cases, the aim is for *BigTech* and *FinTech* operating through digital platforms to no longer position themselves as mere intermediaries but to take responsibility for the content and services offered through their platforms by implementing preventive as well as detective measures (Perez, 2022, p. 42). In both cases, the regulatory instrument chosen is no longer a directive – which has proven to be ineffective, generating fragmentation and disparate criteria – but regulations. This follows the increasing trend towards the use of regulations in recent years to standardise criteria in Europe. In particular, the use of Directives as a tool for legislating on digital services in the past, provoked those countries

such as Germany regulated digital platforms in detail, while other countries were lax or non-detailed enough.

These discrepancies were detected by the tech giants, which settled in the jurisdictions with the least stringent requirements, exemplifying so-called *platform shopping* (Rodríguez de las Heras, 2021, p. 410).

The DMA is a novelty in that it introduces a new figure called a guardian or gatekeeper that is subject to reinforced requirements regarding the prohibition of conditional or exclusive contracting, restrictions on the sale of own products, obligations to facilitate and not block interoperability by third parties through the obligation of access to technological infrastructures classified as central or key, and measures to control possible discrimination via rankings and to facilitate the portability of user data (Zamil & Lawson, 2022, p. 15). This initiative focuses more on operational or tactical issues than on strategic areas, as Gorjón (2022, p. 9) notes. Thus, the Digital Markets Act incorporates different types of measures for each of the different types of actors identified, as outlined in the table below.

<b>Obligations (DMA)</b>	<b>Intermediary services (cumulative obligations)</b>	<b>Data hosting services (cumulative obligations)</b>	<b>On-line platforms (cumulative obligations)</b>	<b>Very large platforms (cumulative obligations)</b>
Transparency reports	Applicable	Applicable	Applicable	Applicable
Requirements on conditions of service to respect fundamental rights	Applicable	Applicable	Applicable	Applicable
Cooperation with national authorities in accordance with their orders	Applicable	Applicable	Applicable	Applicable
Points of contact and, where applicable, legal representatives	Applicable	Applicable	Applicable	Applicable
Notification, action and obligation to provide information to users		Applicable	Applicable	Applicable
Reporting criminal offences		Applicable	Applicable	Applicable
Complaints, redress mechanisms and out-of-court settlement of disputes			Applicable	Applicable

<b>Obligations (DMA)</b>	<b>Intermediary services (cumulative obligations)</b>	<b>Data hosting services (cumulative obligations)</b>	<b>On-line platforms (cumulative obligations)</b>	<b>Very large platforms (cumulative obligations)</b>
Reliable alerts			Applicable	Applicable
Measures against abusive notifications and counter-notifications			Applicable	Applicable
Special obligations for markets, e.g., checking the credentials of third-party suppliers ("know your customer" principle), compliance by design, spot-checks			Applicable	Applicable
Prohibition of advertisements specifically targeted at children and those based on special characteristics of users.			Applicable	Applicable
Transparency of recommendation systems			Applicable	Applicable
Transparency of <i>on-line</i> advertising for users			Applicable	Applicable
Risk management and crisis response obligations				Applicable
External and independent audit, internal compliance verification mechanism and public accountability				Applicable
Freedom of users to opt out of recommendations based on profiling				Applicable
Data exchange with authorities and investigators				Applicable
Codes of conduct				Applicable
Cooperation with crisis responses				Applicable

Table 15 *Obligations of regulated agents under DMA*

Source: Comisión Europea, 2022.

The DMA empowers supervisors with *a priori* control tools, implementing obligations for *BigTech* that operate through platforms and that have high market influence according to both qualitative and quantitative criteria (Rodríguez de las Heras, 2021, p. 413).



In these cases, gatekeepers will be subject to a series of obligations, including (i) prohibition of the use of data obtained from merchants to compete or to give preference to their own products (art.6.2 DMA), as has been the case with Amazon; (ii) limiting users' access to other platforms and enabling data portability (similar to the case of PSD II); (iii) prohibiting the combination of user data from the platform itself and third parties (art.5.2 DMA); and (iv) refraining from hindering interoperability (art.5 and 7 DMA).

As Velasco indicated, the DMA initiative is a positive development in the reorientation of competition law. This proposal still has two unresolved points. The first regards DMA's interaction with different existing regulations. The second point concerns whether the MAD will also be enforceable against claims brought by private entities or individuals that could claim the application of sanctions to platforms (Velasco, 2021, pp. 93-110).

The DSA focuses on reputational risks around *BigTech*, particularly those related to illicit content and reducing platforms' ability to make discretionary choices about the content they display (e.g., product offers or news; Gorjón, 2022, p. 9). The proposed Digital Services Act updates – but does not repeal – the 2000 e-commerce Directive,<sup>161</sup> which was transposed into Spanish law in Law 34/2002 of 11 July on information society services and electronic commerce (LSSI). These regulations required extensive modernisation of a subset of entities regulated under the e-commerce directive, including platforms or *Marketplaces* (i.e., the subset of digital intermediaries is the subject of the new proposed regulation).

These services have emerged because of technological advances, and they have been accompanied by new negative practices, such as the display of illegal or defamatory content, which risks spreading misinformation or bias. In addition, offenders went unpunished as content was removed upon detection without the systematic cancellation or blocking of offenders' accounts. The E-Commerce Directive left loopholes and ambiguities that were filled in through case law, such as the well-known case of Uber (Sentencia del Tribunal de Justicia (Gran Sala) de 20 de diciembre de 2017. Asociación Profesional Élite Taxi contra Uber Systems Spain, SL., 2017) - case and

---

<sup>161</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

recommendations of the European Commission<sup>162</sup>. Thus, over the years it has been defined (i) what a platform is, (ii) when a service is considered neutral, (iii) when it could be assessed as having taken the necessary control measures to be exempted from liability, or (iv) when liability is limited (Perez, 2022, p. 43).

The DSA complements a number of other directives and regulations, which will apply as *lex specialis* to the proposed Digital Services Act. The DSA Regulation itself refers to (i) Directive (EU) 2018/1808 on video-sharing platform providers for audio-visual content and audio-visual commercial communication, (ii) Regulation (EU) 2019/1150 on promoting fairness and transparency for professional users of *online* intermediation services will remain in force, and (iii) Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of consumer protection rules in the Union.

*BigTech* is covered by the Digital Services Act in two ways, both covered in Section V of Chapter III of the DSA: very large online platforms (VLOPs); and very large online search engines (VLOSE). Art.33 of the DSA defines very large online platforms as those on-line platforms which provide their services to an average monthly number of active service recipients in the EU equal to or greater than forty-five million. In these cases, *BigTech* companies are subject to extraordinary measures and supervision, which comprise both internal or governance controls and transparency obligations towards the public. The obligations in relation to governance include the preparation of a risk analysis (with a special focus on systemic risks; art. 34 DSA), risk mitigation measures (art. 35 DSA), verification of the effectiveness and efficiency of controls through external audits (art. 37 DSA), and obligations to hire a compliance officer (art. 41 DSA). The transparency obligations include the disclosure of information relating to recommendation systems and *online* advertising (arts. 26, 17 and 39 DSA) and the publication of reports (art. 42 DSA).

Regarding *BigTech* supervision, this task is centralised at the European level in the Commission and the new European Digital Services Board.

---

<sup>162</sup> Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content *on-line*.

Both regulations are an important step forward in terms of controlling *BigTech* platforms in the EU, but they remain insufficient for several reasons. First, the regulations focus on *BigTech* operating as digital platforms, but not all tech giants provide these services. Second, DMA and DSA address a subset of entities or activities, but the general scope will still be governed by a directive, and therefore discrepant criteria in the general field of e-commerce will remain. Third, these measures are cross-cutting but would not cover risks specific to the financial industry, which would require their own *lex specialis*.

For this reason, both DMA and DSA function as supplementary or partially applicable regulations because they do not regulate all *BigTech* and *FinTech*, nor do they specialise in those entities that provide financial services. Nevertheless, *ex novo* regulatory solutions have been sought following a risk-based approach towards consumers in general, and therefore specific rules and a control environment have been designed to address the risk that *FinTech* marketplaces pose (especially those managed by *BigTechs*).

## VII. REVIEW OF EXISTING FRAMEWORKS

### 1. The digital identity: eIDAS 2

The first question to ask about digital identity is what identity is and where it is defined. According to the Real Academia Española de la Lengua, identity is ‘a set of features of an individual or a community that characterise them compares to others. Awareness that a person or group must be itself and different from others. Fact of being someone or something the same that is supposed or sought’. Identity itself is neither deemed a fundamental right nor defined explicitly in the Spanish Constitution, even if it is the cornerstone of the legislative system (both individual and corporate identities) (González, 2022, pp. 1-20).

Digital identity is the reflection of one’s identity in the digital environment. The digital identity is contemplated in Spain via the *Carta de derechos digitales*<sup>163</sup> (Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, 2021, pp. 5-18). It entails

---

<sup>163</sup> 1. *El derecho a la propia identidad es exigible en el entorno digital. Esta identidad vendrá determinada por el nombre y por los demás elementos que la configuran de acuerdo con el ordenamiento jurídico nacional, europeo e internacional.* (Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, 2021)

not only legal identity, but other components such as social characteristics (the “likes” that the user marks in different social networks) or reputational aspects (González, 2022, pp. 1-20). In this regard, eIDAS mandate pivots around legal digital identity (both individual and corporate).

The Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 to establish a framework for a European Digital Identity (i.e., eIDAS 2) is the result of a combination of (i) low effectiveness of the initial regulatory framework designed around electronic identification and trust services for electronic transactions in the region;<sup>164</sup> and (ii) the development of innovative solutions within this space, such as a cross-border digital identity. This regulatory piece differs from the others reviewed: the scope of the subject matter is cross-sectorial, transcending finance alone. However, it is one of the elements of the Digital Finance Package as well as a key element of the ‘2020 Digital Compass: The European Way for the Digital Decade’ (European Commission [EC], 2021b, pp. 1-21). The Digital Compass sets the future use of a sovereign digital identity wallet as a 2030 objective across the European Union both for individuals and corporations.

The following sub-sections evaluate the deficiencies identified in eIDAS 1 that have informed this initiative, in addition to providing an overview of the regulation, its implications for the financial sector, challenges and points for improvement.

### ***1.1 The basis line: eIDAS 1 effectiveness***

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (known as eIDAS 1) was designed to develop a digital single market that would maintain an adequate level of security and protection for individuals and corporations. It was based on the idea of trust in identification elements that were part of the digital identity, including the possibility to implement and use electronic signatures that would improve business transactions (Llaneza, 2022).

---

<sup>164</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

However, eIDAS 1 did not meet expectations, as reflected in the figures: not all Member States have implemented an eIDAS scheme (only 14 Member States have at least one eID scheme, and only seven of those can be used on mobile devices). Indeed, less than 60% of EU residents have access to eID schemes (European Parliament [EP], 2022, pp. 1-3). In practice, usage of tools such as digital signatures are restricted to certain types of professionals, such as lawyers or notaries, and the schemes are not interoperable. Moreover, the current framework does not allow for the selection of the data shared (create sub-divisions or modules of the digital identity that would be shared with the counterparties, which are currently identified as attributes of the digital identity), nor does it meet current user expectations (computer-based as well as mobile-based trust services).

For this reason, the European Commission performed an impact assessment of the regulation (European Commission [EC], 2021d, pp. 1-86) which identified several high-level problems (European Parliament [EP], 2021, pp. 1-8) . First, the increasing demand (both public and private) for services for trusted identification and the *exchange* of digital attributes is not addressed. Second, current user expectations are not met (cross-border, easy-to-use, friction-free experience). Third, data controls are insufficient given the increased general focus on data management and cybersecurity (mainly in the scope of GDPR and NIS 2). Finally, the regulation permits an uneven playing field that creates fragmentation and barriers due to different standards and perspectives (e.g., the possibility to allow verification of an identity via video).<sup>165</sup>

Because the current eIDAS 1 has several pain points, it is expected that eIDAS 2 will solve the following: (i) fragmentation and lack of interoperability that reduces the use business cases and the attractiveness of the solution; (ii) focus on the electronic signature and not digital identity itself, preventing a comprehensive idea of identity that could include study certificates, driving licenses, or medical data; (iii) linked to the previous point, the current digital identity definition does not fully comply with the data minimisation requirements established in the GDPR as the user has to share all of the eID, not just certain aspects of it (e.g., sharing the full tax ID to prove that a person has reached legal adulthood instead of providing a qualified attestation that confirms that the person

---

<sup>165</sup> In Spain, this has been regulated via Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

is of legal age without disclosing the date of birth or the full eID); and (iv) there is a scarcity of solution providers due to the lack of interest and attractiveness.

### ***1.2 eIDAS 2 overview and its impact on the financial industry***

eIDAS 2 has one general objective and several specific targets. The core objective is ‘to ensure the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions’ (European Parliament [EP], 2022, p. 7).

The specific targets include the following: (i) providing trusted and secure services, (ii) across borders, (iii) protecting full personal data ownership (self-sovereign identity), (iv) ensuring a level playing field across Europe, (v) meeting user expectations and demands, (vi) adapting to the technological environment, (vii) ensuring compatibility with existing and future regulatory pieces that will interact with eIDAS 2 (financial regulation included).

Two of the key novelties in eIDAS 2 are electronic ledgers and the European Digital Identity Wallet, which will need to be available online and offline (there is some ambiguity regarding what offline means and whether it applies in cases where one of the counterparties is online and the other is offline). Both of these additions would support the digitalisation of the financial sector. For example, an eID Wallet would be used for client onboarding as part of the ‘Know Your Customer’ (KYC) procedures. In this way, the information would be provided and verified in a single step. eIDAS 2 also introduces the concept of the electronic ledger, defined in art.1 as ‘a tamper-proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering’. E-ledgers create an immutable audit trail for the sequencing of data records and operations through a combination of timestamping and order.

Although not specifically indicated, this idea is based on distributed ledger technologies and represents an important step towards the adoption of DLT in the financial sector. Even eIDAS 2 contemplates financial-related uses in Recitals 34 and 35, where the regulation indicates that the use of qualified electronic ledgers creates ‘a reliable audit trail for the provenance of commodities in cross-border trade’ and uses related to crypto assets: ‘Use cases that involve crypto assets should be compatible with

all applicable financial rules, for example with the Markets in Financial Instruments Directive, the Payment Services Directive and the future Markets in Crypto Assets Regulation’.

Due to the lack of existing regulation, eIDAS 2 will implement a pan-European framework for standardisation and recognition of trust services supporting e-ledgers. Bonds and securities issuance based on electronic ledgers and the crypto assets business will be based on these future standards, which will require coordination with the various regulations (e.g., a potential PSD III, MiCA, and Pilot). The regulator highlights that the main user of electronic ledgers in 2017 was the banking and finance industry, representing 75% of use cases (eIDAS 2 draft – 2. Legal basis, subsidiarity, and proportionality).

The second key element of eIDAS 2 that impacts the financial sector is the self-sovereign identity (SSI), but the scope of this term is not specified (it is mentioned several times in Recitals and preparatory documents, but there is no specific definition of what is a self-sovereign identity). There is no agreed-upon definition of this concept, and some authors have questioned whether it is self-sovereign (autonomous fully owned, e.g., an IP address or the mobile device used would be attributes of the digital identity beyond the scope of eIDAS which the user may not have decision making power or managing capacity). It is also debated whether an individual has just one such identity or an infinite number given that there are an infinite number of digital attributes that a person generates (Dávila, 2019, pp. 122-124).

Moreover, digital identity is not static but dynamic, and it is therefore difficult to manage or define, thus posing several challenges from the operational point of view. This is reflected in the fact that digital identity under eIDAS has minimum attributes assigned to it but does not aim to list all its attributes, conscious of the lack of cost-benefit that this task would entail.

Allen noted several characteristics that an SSI should encompass:

*(...) the user must be central to the administration of identity. That requires not just the interoperability of a user’s identity across multiple locations, with the user’s consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can’t be locked down to one site or locale.*

*A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying information or facts about personal capability or group membership. (Allen, 2016, pp. 1-15)*

As established in art.1, the scope of eIDAS 2 includes the conditions that Member States must provide and recognise for electronic identification. It also creates rules for trust services, electronic signatures, seals, timestamps, documents, delivery services, web authentication certificates, electronic archiving and attestation of attributes, remote electronic signature and seal creation devices, and electronic ledgers. Moreover, it establishes the creation of a European Digital Identity Wallet.

Regarding how this could look operationally, the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) has provided a potential SSI infrastructure that demonstrates how it could operate (*Bundesamt für Sicherheit in der Informationstechnik, 2021, pp. 1-8*): first, the identity owner or identity holder (the user) would have a wallet with several attributes that have been verified by different authorities (issuers). To get into the eID Wallet, the user must complete a strong user authentication process outlined in eIDAS 2 that is clearly inspired by the strong customer authentication requirements of PSD II. This is likely because, in the future, the eID wallet may also operate as an integrated wallet (e.g., it could potentially operate as a CBDC wallet as well).

The user can then create a digital signature or stamp (in the case of corporations) and can manage the attributes (i.e., the verifiable credentials) so that if a verifier requests it, the user will be able to provide it. To complete the verification, the verifier may require certain technical information (e.g., signature scheme or the public key) that can be stored in a data registry (it could even be a claims registry that would keep information of all the credentials issued). The registry could therefore store cryptographic information as well as additional information. Once the authentication of the attributes is completed and the credential is presented, the verifier can extract the information from the data registry to verify signatures and the authenticity of the keys.



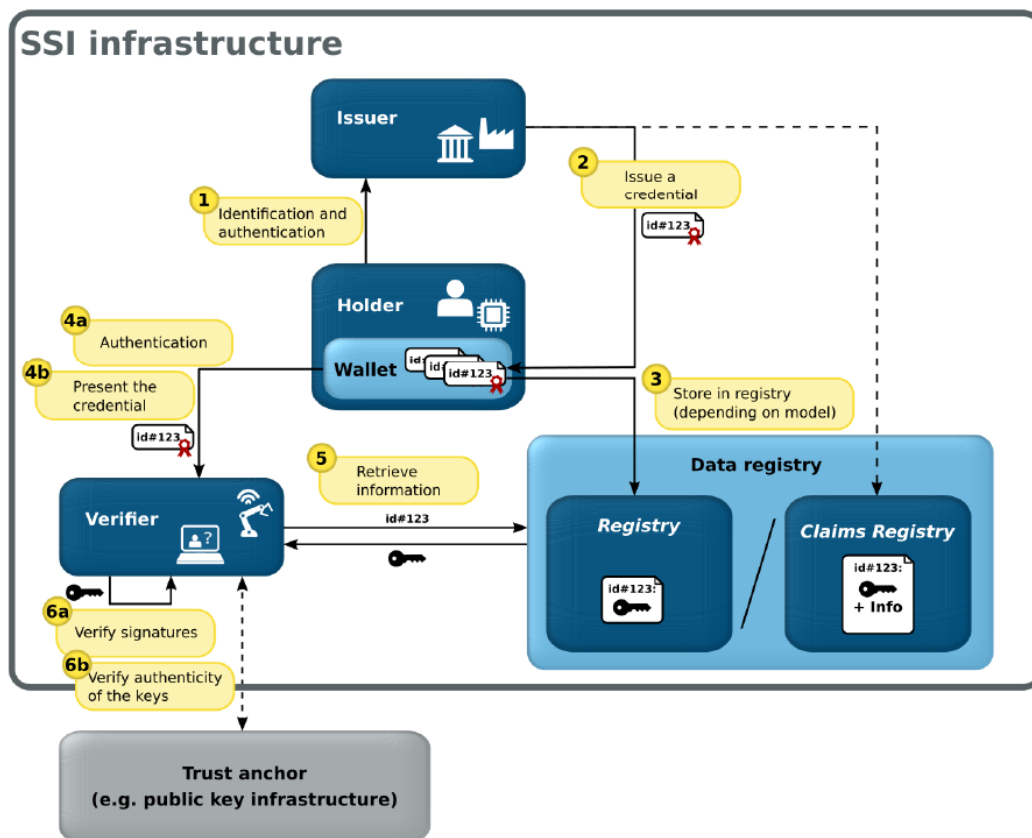


Figure 57 Schematic diagram of the SSI workflow

Source: Bundesamt für Sicherheit in der Informationstechnik, 2021.

Although the DLT-based digital identity is attractive, it is just one of many possibilities. Thus far, Member States have been using solutions with identity cards, such as the Spanish ID (DNI) based on the standards imposed by Regulation (EU) 2019/1157.<sup>166</sup> Using a DLT solution would first require tackling one common and practical problem: if a user loses the private key required to access the eID Wallet, their identity would be lost, with important legal consequences. Hence, a solution is needed to allow users to recover their digital identity if the private key is lost.

There are further questions regarding digital identities that eIDAS 2 does not address, such as the need for an identity tutor role to represent the legal status of those who have guardianship or custody of a minor or a disabled person. Similarly, if just one eID Wallet is issued per person, it is not clear what would happen for individuals with multiple nationalities or with one nationality but residencies in different Member States.

<sup>166</sup> Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (Text with EEA relevance).

Furthermore, eID Wallets for corporations would need to outline legal levels of authorisation or powers of attorney, including whether a joint signature is required to legally bind the corporation. Additionally, it is unclear how will this eID Wallet would interact or coexist with future CBDC Wallets, such as a potential digital euro wallet.

In conclusion, eIDAS 2 is a necessary step toward European digitalisation, but it must be coordinated with different regulatory initiatives, some of which are financial; only in this way will we be able to determine how it will operate in the future.

## **2. *FinTech 3.5* in Europe: PSD II towards PSD III?**

### **2.1 *PSD II overview***

Directive 2015/2336 of 25 November on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC (PSD II), aims to cover both means of payments (the element by which the payment is made) and payment instruments mechanism (Alvarado, 2017, p.3).

PSD I<sup>167</sup> and Regulation (CE) 924/2009 of 16 September 2009 (cross-border payments) focused on promoting a single payment area and served as a cornerstone in the development of the SEPA in terms of homologation and standardisation across the region. However, digital innovations provided by new agents soon caused an impact and rendered EU regulatory payment frameworks obsolete (Peñas, 2020, p. 52). In response, work on PSD II began in 2013.

PSD II includes not only euro payments but all payments in the EU as well as operations for which at least one party is located in Europe, implying a sort of extra-territorial reach (Tapia, 2018, pp. 61-62) that is more commonly seen in Anglo-American regimes (e.g., OFAC rules).

Other key changes include new counterparties with their own specific authorisation regimes and denominated Third Party Providers (TPPs), including a distinction between the new parties of Payment Initiations Service Providers (PISPs) and

---

<sup>167</sup> Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance).

Account Information Service Providers (AISPs) and Account Servicing Payment Service Providers (ASPSPs), or the traditional institutions already identified in PSD I.

PSD II also encompass enhanced controls around payments by (i) implementing new security requirements (i.e., strong customer authentication [SCA] that includes two independent security factors when operating); (ii) increasing requirements around customer protection, disclosure and transparency; (iii) imposing liability regimes; and (iv) enhancing the supervisory regime, including new reporting obligations. Regarding the latter point, under the new regime, both ECB and EBA gain power in relation to authorisation regimes and operational and security risks coverage (Peñas, 2020, pp. 58-60).

## ***2.2 PayTech regulatory framework proposal***

As indicated in the *FinTech 3.0* chapter, not all *FinTech* payment activity is regulated – nor should it be in the case of technological services or ancillary services. However, it is necessary to assess the impact that these unregulated entities have on the supervised entities they interact with either as suppliers or collaborators, as well as possible risks that they present if there is a concentration of service provision or a critical impact on operations.

From the regulator perspective, a balance must be sought between regulatory frameworks and innovation, which requires flexible and agile approaches to processes and time to obtain licences. However, it remains a challenge due to the increasing fragmentation and relocation of payment value chains. Current European regulations (Second Payments Directive and implementing regulations) are insufficient for the reasons described below.

First, the lack of technological neutrality requires the current Second Payment Services Directive to be updated as a Third Payment Services Directive. PSD II was designed based on payment services and infrastructures that use messaging systems like SWIFT. However, since PSD II's publication, more immediate and efficient solutions have emerged, such as the use of Application Programming Interfaces (APIs) and technological solutions based on distributed ledger technologies (DLTs).

Although APIs are already used in banking, they require guidance and clarification from the banking authority (EBA). Despite this, there are still practical barriers to

standardisation that have been the subject of proposals under the consultations carried out by the regulator in 2022 (European Commission [EC], 2022).

Second, the margin of action for information aggregators should be expanded to allow their activities to extend beyond payments to other types of financial products so that users can have better knowledge of their financial situation. This proposal opens the discussion regarding whether the opening of financial services to third parties should be limited to payments and their improvements (a possible Third Payments Directive) or whether there should be an opening of finances in general (in this case it would no longer be a question of open banking but of open finance, with business models that will be evaluated in *FinTech* 3.5). If open finance is considered, a new *ad hoc* regulatory piece would be required (that also addresses payments) that would be a clear indicator of a disruptive environment.

Under the current structure limited to payments, the application of a risk-based approach will be necessary for future regulatory developments related to obtaining licenses, customer protection, internal controls, application of new technologies, and economic stability. The future regulation could open the door for *PayTechs* with limited licenses to be direct members of clearing and settlement chambers (TARGET 2 in the European case), thereby enabling solutions to improve interoperability and transaction times (Asociación Española de *FinTech* e *InsurTech* [AEFI], 2020, p. 77). An even more innovative approach could allow the use of new technologies to dispense with the costs associated with the clearing and settlement houses themselves.

### ***2.3 Towards PSD II or something different?***

Although PSD II is a recent directive and several of its implementing and delegating acts are even more recent,<sup>168</sup> it has rendered obsolete in several regards; this causes us to question whether the ‘future-proof’ requirement is truly accomplished in this regulatory piece. The public authorities have recognised this issue. In October 2021, the European Commission requested advice from the EBA on topics related to PSD II, and from 10 May 2022 to 5 July 2022 a 38-page targeted review of the revised

---

<sup>168</sup> For example, the Adoption of Commission Delegated Regulation supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards specifying the framework for cooperation and the exchange of information between competent authorities of the home and the host Member States in the context of supervision of payment institutions and electronic money institutions exercising cross-border provision of payment services was published in the European Commission web page on 31 March 2021 and is still pending publication as of July 2022.

Payment Services Directive (PSD II) was drafted to collect comments from private sector participants (European Commission [EC], 2022, pp. 1-38).

The main elements under consideration surround strong customer authentication requirements, fraud controls, and application programming interface standardisation needs as possible enablers of future open finance models across industries (mainly to increase data-sharing initiatives).

There are several underlying factors to consider for a potential PSD III. First, there are new business models and agents emerging onto the payments scene that are not covered under existing directive articles. One example of new business model is buy-now-pay-later services, which pose new challenges both to risk management and contractual or consumer protection.

With relation to new agents, MiCA regulation addresses the possibility of *stablecoins* being used as a means of payment (e-money *token*). However, PSD II is currently focused on the use of application programming interfaces and does not envisage the use of DLT or possible challenges to the current payments' directive, such as articles included on the transparency execution side (art.38 to 60 of PSD II) or rights and obligations (art.61 to 100 of PSD II).

The regulation does not include how to cover fundamentals such as consent withdrawal (art.64 of PSD II) or whether the minimum required elements in the framework contracts (art.52 of PSD II) are compatible with *Blockchain* protocols (e.g., the right to block a transaction in case of suspected fraud). Therefore, it is probable that an exemption regime from PSD II similar to the DLT Pilot Regime for market infrastructures may soon become necessary, particularly given the potential arrival of a digital euro (expected to be launched in 2024).

In addition, the instrument used (directive) has not succeeded in providing a level playing field as there have been divergent implementations or interpretations from Member States in level 1 and level 3 regulations. As a consequence, EBA issued several opinions and Q&As that resulted in several adjustments, which posed challenges for the financial services entities covered in the regulation (European Banking Federation [EBF], 2022c, p. 7). This prompts us to consider whether a regulation with direct implementation in the Member States would be a more adequate policy instrument, per the examples of MiCA and Pilot. Regardless of whether a directive or a regulation is used in the next

iteration, it is important that it is flexible enough to be future-proof and compatible with future technologies (European Banking Federation [EBF], 2022c, p. 7).

Moreover, the question is whether European institutions want to continue having a payments-specific regulation (probably considering merging the electronic money Directive<sup>169</sup> with the future PSD III). This is because PSD II was the first step towards open banking in the EU. However, data sharing can take a broader approach to include other types of financial accounts and services, which would unleash a new way of doing business via open finance (European Banking Federation (EBF), 2022c, p. 62). The question is whether an overarching regulation on open finance is required, and PSD III would be *lex specialis* to this future open finance regulation, or whether PSD III should be directly recycled into an open finance regulation and become one of its chapters. An open finance regulation would pave the way towards the Superapps models currently operating in the Asian region (e.g., WeChat), thus allowing competitive business models in Europe.

Finally, there are several aspects of the PSD II that have not worked or that may need review; some of these are listed below.

First, definitions and new concepts: there is no clear distinction between retail and corporate clients for certain elements, such as transparency, SCA, or session timeout, which has led to unnecessary constraints for corporate clients. Moreover, art.4's use of payer, payee, and payment service user includes both natural and legal persons, whereas the consumer definition (art.4 [20]) refers only to physical persons acting for non-professional purposes. Furthermore, this consumer definition conflicts with Law 3/2014,<sup>170</sup> which includes not only physical persons but also certain types of corporations (Peñas, 2020, p. 53).<sup>171</sup>

---

<sup>169</sup> Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance).

<sup>170</sup> Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

<sup>171</sup> «Artículo 3. Concepto general de consumidor y de usuario.

*A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto, son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión.*

*Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial.»*

Articles 2 and 4 of PSD II may need to be adapted to cover cryptocurrency as the current references to the ‘currency of a Member State’ and ‘funds’ would not allow cryptocurrencies to operate as means of payment (Castillo, 2020, pp. 123-162).

There are also other definitions that may need to be reviewed or clarified, such as ‘payment account’ as an ‘account held in the name of one or more payment service users which is used for the execution of payment transactions’ (art.4 [12] of PSD II). According to the Court of Justice of the European Union Case C-191/17,

*(...) Article 4 (14) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC must be interpreted as meaning that a savings account which allows for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account does not come within the concept of ‘payment account’. (Court of Justice of the European Union, 2018)*

Additionally, new terms may need to be included based on the EBA Q&As (e.g., electronic remote payment transaction according to EBA Q&A 2019/4594; EBA, 2022). Moreover, new businesses, operations, and agents need to be considered, including how to approach machine-to-machine transactions, distributed ledger technology, and tokens that could be used as means of payment. Other operational businesses include cash-in-shops where the user has a payment account with access enabled via mobile application. There are agreements with different shops to enable cash deposits and cash withdrawals without having to be clients of the shop or consume services at the shop (i.e., the shop is used as a sort of alternative ATM).

Second, Strong Customer Authentication<sup>172</sup> (SCA) requirements require an important amount of investment, time, and resources for the entities in scope. It was fully rolled out in 2021 (European Banking Federation (EBF), 2022c, p. 6). However, it created friction with customers, and its benefit may have not outweighed its costs for several

---

<sup>172</sup> “‘Strong customer authentication’ means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data’ (Art. 4 (30) of PSD II).

reasons. The SCA requirements are too detailed, leaving entities with little leeway to apply innovative solutions that could bring equivalent security results. For example, the development of behavioural biometrics (European Banking Federation (EBF), 2022c, p. 76) or the digital identity under eIDAS 2.

Third, Fraud prevention measures: PSD II included several fraud articles that aimed to improve management of this type of risk. However, the current trend has been towards authorised push payments, a type of social engineering fraud in which customers input and validate transactions by themselves under the impression that the transaction request launched by the fraudster is legitimate. Hence, following the proposal in DORA, a sort of annual report or information sharing from authorities with regards to fraud typologies under payment services schemes would be a relevant element to incorporate. Additionally, it is questionable whether implementing a two-factor authentication, in which each factor refers to a different category (knowledge, possession, or inherence) make a difference in comparison to implementing two different factors of the same category.

Fourth, Application Programming Interfaces (APIs): the lack of proper standardisation has been one of the main criticisms of this directive, deriving in different API solutions that in practice mean that the third-party provider (TPP) must invest resources into different API requirements to be able to connect with the account servicing payment service providers. Once connected, API quality and the information shared by the financial institutions was not adequate (Johnson, 2022, p. 1). As mentioned, PSD II can be tagged as an ‘API-centric’ regulation that fails to clarify how to proceed with DLT-based solutions. It should be stressed that in 2016, the European Parliament (via Resolution 2016/2007 [INI]) already established the need to review and adapt the payments regulatory framework in lieu of the DLT potential, which is still pending. This included the Payments Accounts Directive, PSD II, and the Electronic Money Directive (European Parliament resolution on virtual currencies (2016/2007 (INI)), 2016, pp. 1-6).

Fifth, Access to payment infrastructures via payment institutions and e-money institutions. The regulator is considering the possibility of these entities becoming direct members of the infrastructure, with access to clearing and settlement systems without the need for a traditional incumbent. This would potentially foster a healthier competitive environment because new participants would not depend on the conditions imposed by



the *incumbents*. However, this measure would need to be aligned with existing requirements regarding guarantees and capital (European Banking Federation [EBF], 2022c, p. 48) to uphold the ‘same activity, same risk, same rules’ principle.

Finally, Incident reporting: as mentioned in the DORA section, the EBA Guidelines on major incident reporting were modified on 10 June 2021 because the original rules were too burdensome and resulted in unnecessary or non-relevant reports being made to the authorities. The first guidelines were developed in 2017 and came into force in January 2018. EBA is also conscious that these 2021 guidelines may be impacted again by the DORA Directive and therefore already foresee a change in the guidelines by 2024 (European Banking Authority (EBA), 2021, p.1).

#### ***2.4 The need for a dialogue between MiCA and the Payment Services Directive***

MiCA establishes several categories of *tokens* that are covered under its proposal. Two of these (asset-referenced *tokens* and e-money *tokens*) are payment *tokens*, understood as a mean of payment that is generally or socially accepted for transactions between private counterparties according to the social theory of money (Ciraolo, 2022, p. 94). Specifically, MiCA establishes that e-money *tokens* should be considered equivalent to electronic money (art.48.2 of MiCA), again applying an analogy principle. In this case, instead of the ‘same activity, same risk, same rules’ principle, we would consider the approach as using the ‘same service or use, same risk, same rules’ principle. Thus, this type of token will be subject to the Electronic Money Directive and, consequently, to the PSD II for those elements not specifically addressed in MiCA, which relate mainly to transparency, customer protection, and service provider liability.

Both, the Electronic Money Directive and PSD II are grounded on traditional entities and operations. As such, exemptions to their requirements would need to be covered by MiCA. Otherwise, it will become necessary to revamp those regulatory pieces in the coming years. As indicated by Ciraolo,

*la extensión a los criptoactivos con función de pago de reglas desarrolladas asumiendo un contexto operativo diferente como punto de referencia puede generar (...) diversas dificultades interpretativas y de aplicación, que surgen de un léxico técnico-jurídico cuyo uso (...) puede parecer de alguna manera ‘forzado’.* (Ciraolo, 2022, p. 101)

Clarification of which new crypto assets are considered ‘means of payment’ and therefore subject to PSD II is also needed. Even bitcoin has been considered a means of payment (Court of Justice of the European Union, 2015).<sup>173</sup> Thus, clarification is needed regarding specific categories of tokens (i.e., only e-money tokens, extensions of asset-referenced tokens, or beyond) before developing the next regulatory piece.

Moreover, other technical or tactical elements should be synchronised or exempted, such as (i) pre-contractual and post-contractual obligations; (ii) the interaction or relationship between the MiCA white paper requirements and the contractual requirements of PSD II (art.52 of PSD II); and (iv) the roles, responsibilities, and liabilities of new participants (crypto asset services providers), which appear to go beyond those of PSD II.

Finally, PSD II review may not be unfolding into a PSD III but into a possible direct regulation or even a much broader concept, such as an *open finance* potential regulation. Otherwise, the regulator would need to design a separate regulatory piece to address *open finance*, with payments a sub-category. Additionally, interaction with different regulations and initiatives – including eIDAS, CBDC, MiCA, DORA, AML, and GDPR as well as instant, cross-border, and atomic payments – should be considered to avoid inconsistencies.

---

<sup>173</sup> According to this court ruling, ‘The “bitcoin” virtual currency, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment, or a transfer. Moreover, unlike a debt, cheques and other negotiable instruments referred to in Article 135(1)(d) of the VAT Directive, the ‘bitcoin’ virtual currency is a direct means of payment between the operators that accept it.’ (...) “Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions.’

## CHAPTER VIII. CONCLUSION

Although there is no agreed-upon definition for what *FinTech* is, this thesis has analysed *FinTech*'s key features and has reached a description broad enough to capture this dynamic phenomenon. *FinTech* is not a type of entity (*FinTech* firm) but rather denotes the **development of technological innovations in digital environments with a real or potential material impact on the financial industry and therefore on its infrastructures and participants** (consumers, entities, financial institutions, and authorities).

This research has investigated the general hypothesis that *FinTech* disruption is currently exceeding the boundaries of the regulatory and supervisory frameworks at the present, leading to legal gaps at various levels (local, regional and global). Accordingly, there is a clear need to reconsider the current way for regulating and supervising the financial activities with innovative components. This primary hypothesis was backed by several secondary hypotheses to reach a holistic understanding of the complex panorama of *FinTech*.

Based on definition designed, *FinTech* is a form of innovation whose impact on the financial sector is not recent – it has been manifesting for decades, starting in 1866. Accordingly, *FinTech* has undergone a range of phases. *FinTech* 1.0 and 2.0 were mainly evolution phases, whereas *FinTech* 3.0, 3.5, and 4.0 were disruption phases that caused a paradigm change due to several factors. *FinTech* 3.0's main disruptive factors are the openness of payment data via technology, cross-border reach, and the emergence of external actors. Some of these factors have the potential to cause systemic impact, such as *BigTechs*. *FinTech* 3.5, led by emerging regions, absorbed the above characteristics, and increased the number of innovations across financial services, not limiting them to the payments sphere. Moreover, there is an increasing number of models and services that are not regulated or that do not fit into the existing regulatory and supervisory structures, creating both regulatory and supervisory gaps in a strategic sector. This issue increases with hybrid models that re-bundle financial activity with non-financial activity or with the 'as a service' business, thereby creating confusion and discussion around whether they entail a sort of license assignment.

Finally, the *FinTech* 4.0 phase has brought absolute disruption by considering the code as the law and the possibility to prescind traditional third parties from performing

financial business. Moreover, businesses based on *FinTech* 4.0 have no geographical boundaries and can operate globally without being attached to any particular jurisdiction; as a result of this, they cannot be censored. *FinTech* 4.0 brings its own social structure (decentralised autonomous organisations), its own financial structure (decentralised finance) with its own money and assets (crypto and digital assets), agents (oracles), as well as its own new digital worlds (Metaverse), all of which rest on the pillars of a new technology. However, this thesis debates whether these are real decentralised models or whether we are witnesses of the shift from traditionally regulated third parties (financial institutions) or unknown non-regulated third parties (the code developers or DAO material decision-makers).

Furthermore, the *FinTech* 4.0 era brings the disruptive element of the capacity of non-banking actors (entities or even individuals) to issue their own digital version of value (tokenised assets) or native versions of value (crypto assets and *stablecoins*), which can operate and transfer value without a central bank or a financial institution. As a reaction to this threat and to protect the monetary policies of EU Member States, countries are exploring the possibility of issuing their central bank digital currencies. However, this option envisages issues from different aspects, such as the impact on traditional finance actors or inflation.

Therefore, the secondary hypothesis 1 is confirmed, as the introduction of emerging technologies on traditional finance implies a clear disruption and has prompted the need to adapt the regulatory approach in the EU.

Also, it has been proven that the concept of trusted third party has shifted from traditional actors (central banks and *incumbents*) towards code-driven trust actors that challenge the established norms, requiring a new approach on this cardinal element (secondary hypothesis 2).

Analysing these disruptive patterns reveals that the number of innovations and new counterparties is so abundant and heterogeneous – and that these have emerged over such a short time (2008 onwards) – that the regulation has not been able to cope, resulting in unsatisfactory proposals that are born outdated, as evidenced by the analysis of existing core regulatory initiatives in the European Union. Hence, financial regulation is facing a permanent gap because the regulatory processes cannot cope and have not moved at the

same pace as innovation. Indeed, the regulatory vacuum has been increasing over the last few years (secondary hypothesis 3).

Similarly, supervision is subject to jurisdictional limits as well as issues with subject matter scope. These boundaries are exceeded by agents, activities, and geographies, rendering the existing supervision partial and inefficient. Inadequate or partial oversight of activities and agents underscore the need for fresh approaches that can guarantee an effective control over constantly evolving technological innovations (secondary hypothesis 4).

In the analysed scenarios, the supervisor is expanding the interpretation of the law. In some cases, it could be argued that its mandate, by temporary applying the analogy to the focus of the problem, is similar to what a judge does when faced with a regulatory gap based on the principle of ‘same activity, same risk, same rules’. However, this thesis has determined that this principle is insufficient as *FinTech* is usually a different activity that poses different inherent risks.

New supervisory innovations such as the regulatory sandbox are not a strategy but a mere instrument of the supervisor to identify regulatory gaps provoked by *FinTech* and separate, supervise, learn, and re-interpret existing regulatory frameworks for amendment to address the issue. However, this solution is not scalable, and certain circumstances may not even be attractive to private sector participants.

This leads to the conclusion that the existing regulatory and supervisory arrangements no longer work for financial innovation models, and therefore a new solution should be sought (secondary hypothesis 5).

This study observes that *FinTech* encompasses such a plethora of activities and counterparties that a single solution is not enough, and the optimum outcome depends on the activity or phenomena evaluated. Due to the borderless characteristics of these new activities, a risk-based approach should be considered from the regulatory perspective, trying to incorporate a technological compliance by design approach rather a traditional regulatory perspective (secondary hypothesis 6). Also, a cooperative framework would be needed.

Actors such as *BigTechs* and new asset classes such as significant *stablecoins*<sup>174</sup> render the jurisdictional mandates of European Union regulators and supervisors ineffective. As such, global minimum standards and a coordinator-of-coordinators model would be ideal. It is also evident that this proposal has a low probability of success given that governments are not capable of reaching global agreements on key topics such as health during special crises. Thus, it is highly improbable that can reach adequate compromises in the financial space.

It can be argued that a global model (coordinator-of-coordinators model) implies ceding sovereignty, but these new actors and activities already entail an undermining of sovereignty which cannot be solved at a purely local or regional level. Another challenge is the continuous development of new activities that quickly gain importance and that are difficult to manage. These *FinTech* models often interact with traditional finance players as service providers, agents, or partners. For this reason, a possible solution would be to delegate the supervision via third-party control regulations for supervised entities.

The most technologically advanced and decentralised business models may need to be treated using technological solutions such as minimum compliance by design requirements in the protocols, coding or in the blockchain validators or miners. This alternative would offer minimum controls independently of whether a jurisdiction or supervisor can be identified. These models cannot be driven by analogy solutions because it is sometimes not the same activity, and on many occasions, it is not the same risk (the technological NDA prevents consideration of equivalent risk, and there is an unidentified country risk for decentralised models). Therefore, a different regulation would apply (not the same activity or not the same risk = different regulation). In these situations, an *ad hoc* regulation may be required due to the existence of a regulatory gap.

A regulatory gap is the lack of fit-for-purpose regulations to govern. In this case, regulations are missing for the *FinTech* industry and activities. Due to the borderless nature of the phenomenon, it could even be expanded to the lack of consistent regulations across different regions, which causes a sort of global regulatory arbitrage. The absence of certainty causes agents operating in the *FinTech* to have different understandings of what is allowed or prohibited (i.e., different reasoning regarding whether an activity is allowed because it is not regulated or whether it is prohibited because it is not regulated).

---

<sup>174</sup> Also known as systemic *stablecoins* or significant *stablecoins* under MiCA.

Regulators and supervisors encounter the challenge of how to face these new realities. Not regulating can impact market stability and produce an uneven playing field between *incumbents* and new players. What's more, it has also been used as an opportunity to criminalise or sanction activities. However, excessive controls can hinder innovation. For this reason, it is key that the authorities keep up with these rapidly changing activities and develop effective and proportionate regulatory and control frameworks.

Regarding regulation, this thesis proposes principle-based regulation for *ex-novo* laws that should be grounded on the following premises. First, the need for a new regulation emerges only if the 'same activity, same risk, same rules' principle cannot be upheld. Second, the regulation should be proportional to the types of business, volumes, complexity, and markets. This idea should also be interlinked with the risk-based approach (i.e., those activities that pose higher risk will be subject to enhanced scrutiny). Therefore, the regulator must prioritise activities that are more tangible or material to the market.

Third, the concept of delegation entails the recognition that the supervisor cannot control each one of the casuistries that continually arise and therefore should delegate to private sector actors. These actors would then be responsible for performing due diligence on their respective *FinTech* counterparties. Fourth, technologically neutral regulation is needed to cope with innovations, but in certain cases technologically specific regulation may be required (e.g., smart contract regulation). Finally, the regulation needs to be future-proof and therefore cannot include the level of detail found in current level 1 initiatives in the European Union.

These principles have not been considered in the existing *FinTech* regulatory initiatives, some of which are already outdated or run the risk of creating fragmentation in the European Union. One example would be the DLT Pilot Regime, which is presented as a sort of sandbox solution for the European Union in market infrastructures. However, the DLT runs the risk of generating multiple venues with different models, rulebooks, and infrastructures. Moreover, regulations such as MiCA have required years of preparation and require 12 to 18 months for implementation. During this time, new realities have surfaced that will not be regulated for a long period of time. This causes high-risk

scenarios such as the one described in relation to the Russia-Ukraine War and the travel rule regulations in Europe.

Moreover, supervisors may need to consider new indicators to evaluate whether they qualify as adequate to monitor a business model or activity. New solutions such as *SupTech* and embedded supervisions need to be embraced. Crucially, both, regulators and supervisors will require a profile change towards techno-law professionals to be able to fully understand the potential and risks for new business models and to propose controls that are compatible with emerging technologies.

*FinTech* is incessantly evolving, and its continuous expansion creates countless avenues for future investigation. One path would be how this interaction with *FinTech* activities impacts the private sector from a legal or compliance perspective, especially in terms of which kinds of industry standards would be required for areas that have been ignored in European regulations.

Innovation has come and will continue. We all need to embrace the potential of disruptive models that we often cannot define or delimit. At the same time, we must develop solutions for how to bring this potential to the market and the public in a safe way. To achieve balance, it is not possible to ban or prohibit these activities. Both the public sector and private sector need to upskill to learn how to thrive in this new world.

This thesis has evidenced how fragmented regulatory and supervisory models have lost effectiveness because of the paradigm shift in financial markets. Global operations overflow the supervisory perimeters, making them less effective. Consequently, it is worth considering a combination of elements to be considered to address the issue, which, for the purposes of this proposal, were structured from a global sphere to a micro sphere (private or self-regulatory).

The global operational capability of *FinTech* innovations, especially crypto assets and DeFi, calls for the establishment of a regulator of regulators or coordinator of regulators, with the ability to set global minimum standards and, perhaps, oversee materially global businesses, whose risk analysis cannot be complete without a global view. As an example, the operations of tech giants, global stable cryptocurrencies or DeFi models would fall under this scope of oversight.



In the regional field, regulations suffer from a clear need for greater agility and flexibility. This could be achieved through principle-based regulations, the details of which would be established through *rule books* with time-optimized regulatory processes. The principles would be global (more immutable), while the rule book would be a new form of law with a strong technological component (a sort of technological law). However, an inadequately coordinated regional approach would lead to the risk of regulatory arbitrage, as is currently happening. Therefore, the author agrees with Ibáñez's (2018) statement regarding *Blockchain* technology in general, stating that "This reality exposes the shortcomings of the lack of legal community at the cross-border level (...)" (Ibáñez, 2018, p. 174).

Regarding the licensing facet, this should also be reviewed to allow for lighter or scaled licenses, with approval times in line with the new realities.

On the supervisory side, the implementation of *SupTech* is clearly the way forward for supervisors through integrated or real-time supervisory models, and the use of *big data* and AI for trend and risk identification. Understanding what is happening in the market and how it is progressing can be achieved through so-called financial innovation enablers (innovation hubs and *sandboxes*), which are discussed below. According to Muñoz (2017), "the legal approach requires a deep knowledge of the technological functioning for the warning of potential conflicts and deprotection of interests that such technology may cause" (Muñoz, 2017, p. 4). This need is transferred to the supervisory environment in the same way.

Although there are measures to be implemented from a supervisory perspective, these will require some complementarity from the private sector. Due to the granularity and constant change of *FinTech*, it is sometimes unclear whether the business offered is financial or purely the provision of technology services, making it necessary to delegate supervisory or control functions to the private sector.

This means that, in the case of *FinTech* organizations operating under traditional (centralized) corporate forms, it is necessary to have internal control figures, such as audit, risk or compliance, similar to the requirements that occur in traditional models. In addition, the principle of proportionality could be applied, which means that, in the case of small organizations, these figures could be concentrated in a single internal control entity.

These control functions required of regulated entities (traditional financial institutions, *FinTech* and *TechFin* that are fully or partially regulated) would extend their control capacity over those providers to which they outsource critical functions or that provide services classified as key, which would represent a second level of supervision, which could be considered indirect.

Under the scenario of fully decentralized operations, the code is the law (in *Blockchain*, we speak of cryptography as law, and, therefore, of a *cryptographic lex*). In that sense, the need for inclusion of arbitration elements or claiming power in the very protocols, platforms or white papers of products and services should be raised. Smart protocols and contracts would encompass not only the activity itself but would also operate as a sort of automatic judges in the first instance, whereby courts would intervene in case of damages or serious failures of *smart contracts* (de Filippi and Wright, 2018, pp. 173-204).

One could even consider self-regulation formulas whereby *Blockchain* designs or developments would follow certain standards (e.g., ISO) or display certain fields required for token issuance. In that way, users would be able to understand the risks and compare *tokens*, as well as distinguish standardized *tokens* from those that may turn out to be fraud. Indeed, it could come to be considered control elements within Ethereum's own ERCs or in the validation of blocks (rules in validator nodes), which would function as a sort of control-by-design or compliance-by-design model, in line with the doctrine's comments regarding the need for certain legality tests in proofs of concept of *FinTech* models (Muñoz, 2017, p. 4).

One can follow this line of reasoning and extend it to the application of *Blockchain* in solutions in the financial industry. Because many of the developments are of a decentralized type (*peer to peer*), the possibility of evasion of traditional type regulations and supervisors is high (de Filippi and Wright, 2018, p. 104), and the cost of pursuing non-compliance is excessively onerous. For this reason, the proposed solution of establishing criteria from the very design of the smart contract could be considered a viable alternative, of a preventive nature.

The author agrees with the solution proposed by de Filippi and Wright (2018, p. 104), by means of which an incentive system could be developed for those participants or operations that are processed following the proposed standards, as well as creating natural barriers with respect to those protocols that do not comply "by design". However, this

preventive solution is only partial and has certain limitations. First, the global nature raises the question of which authority would be qualified to develop these standards, since it would require in-depth knowledge of both the technology and the standard, encompassing the agreement of all governments, which, at present, is highly unfeasible. Moreover, imposing standards on the design of smart contracts or *Blockchain* standards could lead to undesired results or a limitation of innovation.

Second, only a subset of rules would be suitable through this *cryptographic lex*, since, being based on *Blockchain*, they would be deterministic and therefore highly rigid, leaving little room for interpretation. While the use of oracles could have the potential to give some flexibility to these rules in the code, these would be limited, so traditional regulation and classical supervision is demanded as a complement and risk mitigator. By virtue of this, the position of this thesis is that, at present, the *cryptographic lex* is a complement that, while gaining more and more weight, does not have the capacity to replace traditional regulations and supervision models.

Thus, as can be seen, the vision of *FinTech* supervision would be a combination of global and public as well as decentralized and private elements, creating an integrated and collaborative control context.



## **ANEXOS**



## ANEXO I. GLOSARIO

Abreviatura	Significado
<i>Airdrops</i>	Repartos y asignaciones gratuitas de criptoactivos, por lo general con fines promocionales y de marketing para dar a conocer el <i>token</i> a la mayor cantidad de público posible y comenzar la circulación de este (Bit2me, 2022).
<i>BigTech</i>	Entidades de gran tamaño que, por lo general, provienen del mundo tecnológico, y que, en su gran mayoría, se basan en un modelo de negocios de plataformas <i>online</i> .
<i>Blockchain</i>	<i>Blockchain</i> o cadena de bloques es un tipo específico de DLT que forma bloques, unidos unos a otros a través de claves criptográficas ( <i>hash</i> ) como forma de comprobación que la información no es manipulada. Puede definirse como “un libro de registro inmutable que contiene la historia completa de todas las transacciones que se han ejecutado en la red, a cada participante se le llama nodo, que en realidad viene a ser un ordenador más o menos potente” (Ortega, 2019, p. 24).
<i>Coin scraping</i>	Método de redondeo en compras y transacciones con el fin de ahorrar pequeñas cantidades.
<i>CompTech</i>	Innovaciones tecnológicas aplicadas a <i>compliance</i> (cumplimiento normativo).
<i>Copy trading</i>	Posibilidad de que otros usuarios puedan replicar o copiar la estrategia que alguien que sea considerado como un experto por la comunidad y que esté operando en una plataforma de inversión ( <i>WealthTech</i> ).
<i>CrediTech</i>	Tecnología aplicada a actividades de financiación.
Criptoactivos	“Representaciones digitales de valor habilitados por la criptografía y la tecnología de registros distribuidos” (Su, 2020, p. 2-24). “Una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar” (art. 3.1 (5) MiCA)
Criptomonedas Criptodivisas	o Subconjunto de criptoactivos divisibles, intercambiables, portátiles y consumibles.
<i>Crypto trading</i>	<i>wash</i> Práctica de alteración de precios, mediante la activación de volúmenes de compras y ventas entre direcciones cripto que pertenecen a empleados, personas relacionadas o la el propio <i>exchange cripto</i> .
<i>Crowdequity</i>	Solución de inversión entre iguales ( <i>peer to peer</i> ) mediante el uso de la tecnología Modelo que "permite a las empresas poder adelantar el cobro de sus facturas a través de inversores particulares que adelantan el importe de estas y a cambio obtienen el derecho de cobro al vencimiento de la factura" (Asociación Española de <i>FinTech</i> e <i>InsurTech</i> [AEFI], 2022, pp. 19-20).
<i>Crowdfactoring</i>	También denominado micro mecenazgo, financiación colectiva, financiación en masa o por suscripción, consiste en la financiación (capital o pasivo) por medio de plataformas digitales, que permiten poner en contacto a los promotores de los proyectos con sus potenciales inversores o prestamistas.
<i>Crowdfunding</i>	Solución de financiación o préstamo entre iguales ( <i>peer to peer</i> ) mediante el uso de la tecnología.
<i>Crowdlending</i>	Billeteras digitales cripto gestionadas por un proveedor de servicios, son custodial o <i>hosted wallets</i> (Wharton School, Digital Asset Project, World Economic Forum, 2020). A su vez, pueden existir dos formatos, <i>hot storage wallet</i> (billeteras que están en línea) y <i>cold storage wallet</i> (billeteras <i>off line</i> ).
<i>Crypto wallet</i>	<i>custodial</i>
DAO	<i>Decentralized Autonomous Organization</i> . Organización Autónoma Descentralizada.
DApp	<i>Decentralized application</i> . Aplicación descentralizada.
<i>Dark DAO</i>	DAO oscuras. Agrupaciones (carteles) que adquieren <i>tokens</i> o compran votos <i>on-chain</i> de forma oculta con el fin de adquirir capacidad decisoria suficiente como para que la DAO atacada tome decisiones en favor de los intereses de la dar DAO debido a la pérdida de control de <i>tokens</i> de gobernanza durante sus votaciones.
Diem (ex-Libra)	Proyecto fallido de <i>stablecoin</i> global, sistémica o significativa liderado por Facebook (actualmente Meta).
<i>Fiat</i>	Dinero de curso legal.
<i>FinTech</i>	Desarrollo de innovaciones tecnológicas en entornos digitales con impacto material real o potencial en la industria financiera, y, por ende, en sus infraestructuras y participantes (consumidores, entidades, instituciones financieras y autoridades).

Abreviatura	Significado
<i>flash loans</i>	Concesión del préstamo sin ningún requerimiento de identificación, análisis de crédito o colateral, siempre y cuando las cantidades sean devueltas dentro del mismo bloque de Ethereum (la operación se abre y cierra en una misma transacción) (Aave, 2022, p.1)
<i>fork</i>	Casos de fraccionamiento de la cadena de bloques (separación), dando lugar a dos monedas por cambios en el código. En el escenario del <i>soft fork</i> los <i>softwares</i> son compatibles, pero en el <i>hard fork</i> no lo son (CryptoCurrency Facts, 2021).
<i>future-proof</i>	A prueba de futuro
<i>gold plating</i>	Interpretaciones diferentes por parte de cada jurisdicción local, pudiendo incluso, regular en determinados aspectos de forma no coordinada añadiendo barreras o requerimientos.
<i>hash</i>	Claves criptográficas incorporadas a los bloques. Operación criptográfica que genera identificadores únicos e irrepetibles a partir de una información dada (Bit2me, 2022a).
<i>home supervisor</i>	<i>state</i> Autoridad encargada de la supervisión en la jurisdicción de origen (jurisdicción de la entidad cabecera del grupo). Cuenta con responsabilidad principal de autorizar y supervisar al grupo financiero.
<i>host supervisor</i>	<i>state</i> Autoridad encargada de la supervisión en una jurisdicción de destino (jurisdicción en el que el grupo financiero ha establecido sucursales o realiza actividades cross-border- sin presencia física vía pasaporte europeo).
<i>Incumbent</i>	Instituciones financieras ya establecidas (instituciones financieras tradicionales o <i>TradFi</i> ).
<i>InsurTech</i>	Innovaciones tecnológicas aplicadas al sector seguros.
<i>legal wrapper</i>	Envoltorio o forma legal dada a las organizaciones autónomas descentralizadas (DAO).
<i>LegalTech</i>	Innovaciones tecnológicas aplicadas al sector legal.
<i>level playing field</i>	Igualdad de condiciones.
<i>Marketplace FinTech Marketplace</i>	<i>o</i> Comercio (generalmente aplicación o plataforma) que oferta diversos servicios de terceros (financieros o no).
Neobanco	<i>PayTech</i> de licencias limitadas o sin licencia propia que se apalancan en terceros (González de Audinaca Zorraquino, 2019), reduciendo sus costes y tiempo de entrada al mercado, a la vez que pueden ofrecer otro tipo de servicios complementarios a sus usuarios, resultando en una aplicación o web cuya apariencia es similar a la de un banco debido a la variedad de productos que se ofertan, siendo parte propios y parte locales.
<i>Non-custodial wallet, unhosted wallet o private wallet</i>	Las billeteras son <i>software</i> de interfaz de usuarios empleados para gestionar los criptoactivos en una Blockchain. Existen dos tipos dependiendo de quién tiene control de las claves privadas: si es la propia persona, se trata de <i>unhosted wallets</i> o <i>non-custodial wallets</i> .
<i>Off chain</i>	Término empleado para hacer referencia a sucesos o actividades fuera de la cadena de bloques.
<i>On chain</i>	Término empleado para hacer referencia a sucesos o actividades en la cadena de bloques.
<i>Open Banking</i>	Banca abierta (apertura de APIs de pagos a terceras partes).
<i>Open Finance</i>	Finanzas abiertas (apertura de APIs de todo tipo de servicios financieros a terceras partes).
<i>PayTech</i>	Innovación tecnológica aplicada a las actividades relacionadas con pagos.
<i>Piggy bank</i>	Versión digital de la clásica hucha. En este tipo de aplicativos los usuarios establecen unos objetivos de ahorro, en los que, por lo general se indica el propósito, cantidad y tiempos. La forma de ahorro puede aplicarse <i>coin scraping</i> (redondeo). REGLAMENTO (UE) 2022/858 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) n.o 600/2014 y (UE) n.o 909/2014 y la Directiva 2014/65/UE (Texto pertinente a efectos del EEE).
Pilot	
<i>Pump and dump</i>	Ventas de grandes volúmenes de <i>token</i> que provocan descensos drásticos del precio de estos, llevando a pérdidas las inversiones del resto de clientes.



<b>Abreviatura</b>	<b>Significado</b>
<i>RegTech</i>	Innovación tecnológica aplicada a las actividades regulatorias (supervisión y cumplimiento).
<i>Retail CBDC</i> o <i>rCBDC</i>	Moneda digital de banco central enfocada a público general (minorista).
<i>Robo-advisors</i>	Programas que permiten la automatización del asesoramiento y operaciones accesorias al mismo (Brummer, 2020).
<i>Rug pull</i>	Operativa por la que los <i>tokens</i> se diseñan con fines de engaño (incluso se suelen copiar gran parte de la programación de <i>tokens</i> existentes). El <i>token</i> es listado en plataformas de intercambio cripto y se promociona a través de redes sociales, empleando cuentas ficticias o bajo seudónimos. Posteriormente, los promotores retiran sus <i>tokens</i> (obtienen ganancias en Ethereum o monedas estables), provocando drásticas bajadas en los precios, y por tanto pérdidas en inversores minoristas o ajenos a la estafa.
<i>Sandbox</i> o <i>regulatory Sandbox</i>	puente que permite a las entidades privadas examinar en producción sus modelos novedosos a la par que las autoridades alcanzan un mayor entendimiento de estos, siendo capaces de este modo de asesorar sobre la posible necesidad de nuevas interpretaciones de la regulación existente o el desarrollo de normativas <i>ad-hoc</i> .
<i>Scale up</i>	Estadio intermedio de una entidad, más allá de la fase de capital semilla y anterior a la fase de Unicornio o <i>BigTech</i> .
<i>Social trading</i>	Plataformas en las que los inversores se ponen en contacto entre sí o con traders profesionales, pudiendo existir diferentes modelos de negocio, que van desde el intercambio de información y opiniones de carácter financiero hasta la emulación de estrategias de inversión de terceros de forma automática.
<i>Stablecoins</i>	Criptoactivos de emisión privada diseñados para solventar los riesgos de volatilidad de los que monedas como Bitcoin mediante sistemas de referencia a activos, derechos, divisas, cestas de éstos, pudiendo estar garantizados o anclados vía algoritmos.
<i>Staking</i>	Adquirir criptoactivos y bloquearlos (pignorarlos) con fin de recibir ganancias o recompensas (ya sea en dinero <i>fiat</i> o en criptoactivos) (Bit2me, 2022a).
<i>Start-up</i>	Entidad de reciente creación en fase de capital semilla.
<i>SuperApp</i>	“Ecosistema cerrado de muchas aplicaciones que la gente usaría todos los días porque ofrecen una experiencia fluida, integrada, contextualizada y eficiente” (Infopulse, 2019, p. 1).
<i>SupTech</i>	Innovaciones tecnológicas aplicadas a las actividades de supervisión.
<i>TechFin</i>	Entidades de origen tecnológico que extienden sus actividades al sector financiero mediante el empleo de soluciones digitales o de alto contenido tecnológico.
<i>Tokens</i>	Fichas basadas en tecnología <i>blockchain</i> empleadas para distintos propósitos.
<i>Travel rule</i>	Información que ha de acompañar a las transferencias, actualmente en proceso de extensión a criptoactivos bajo el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.
<i>Tumblers</i> o <i>mixers</i>	Se trata de servicios ofrecidos para aumentar la privacidad y perder el rastro de los criptoactivos mediante la mezcla de fondos de criptodivisas (con origen ilícito) con otros, con la intención de confundir el rastro con la fuente original de los fondos.
<i>WealthTech</i>	Innovación tecnológica aplicada a las actividades de inversión.
<i>White paper</i>	Documento informativo requerido para la emisión de criptoactivos bajo MiCA.
<i>Wholesale CBDC</i> o <i>wCBDC</i>	Moneda digital de banco central enfocada a sector mayorista (pagos interbancarios).
<i>Yield aggregator</i>	Agregadores de rendimiento.



## ANEXO II. ANÁLISIS DE DEFINICIONES *FINTECH*

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
España	Autoridad	CNMC (Comisión Nacional de los Mercados y la Competencia)	2018	Aplicación disruptiva de las nuevas tecnologías al sistema financiero, puede representar importantes ventajas desde el punto de vista de la regulación del sistema financiero	Innovación	Sí	Amplio	E/CNMC/001/18 Estudio sobre el impacto en la competencia de las nuevas tecnologías en el sector financiero ( <i>FinTech</i> ) <i>The Future of FinTech: Integrating Finance and Technology in Financial Services.</i> Palgrave Macmillan (Palgrave Studies in Financial Services Technology)
Italia	Academia	Nicoletti Bernardo	2017	" <i>FinTech</i> " en un sentido amplio se refiere al uso de las TIC para brindar servicios financieros	Innovación	No	Oferta de servicios financieros (B2C)	<i>FinTech</i> desde la perspectiva de la promoción de la competencia Financiación Digital y su Incidencia en el Gobierno Corporativo
España	Academia	Jose Luis Rodríguez	2019	Aplicación disruptiva de las nuevas tecnologías de la información y las telecomunicaciones (TIC) al sistema financiero	Innovación	Sí	Amplio	
España	Academia	Ana Felicitas Muñoz	2019	Aplicación de innovaciones futuro de la digitalización en el contexto financiero	Innovación	No	Amplio	
Italia	Academia	Alessandra Tanda, Cristina-María Schena	2019	<i>Companies operating in financial intermediation mainly through technological or digital solutions</i> (Empresas que operan en la intermediación financiera)	Entidad	No	Oferta de servicios financieros (B2C)	<i>FinTech, BigTech and Banks</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
España	Academia	Francisco de Audicana González Zorraquino	2019	principalmente a través de soluciones tecnológicas o digitales) Ofrecimiento de productos y servicios financieros en un entorno digital por medio de empresas o aplicaciones que utilizan la tecnología para su desarrollo y potenciación, sirviendo a su vez, esa misma tecnología, de empoderamiento del usuario/consumidor digital, entendiéndose como tal, a la persona física que actúa en un ámbito ajeno a su actividad profesional en un entorno digital <i>FinTech is defined as encompassing advances in technology and changes in business models that have the potential to transform the provision of financial services through the development of innovative instruments, channels and systems. (FinTech se define como el conjunto de avances tecnológicos y cambios en los modelos de negocios que tienen el potencial de transformar la provisión de servicios financieros a través del desarrollo de instrumentos, canales y sistemas innovadores.)</i>	Innovación	No	Oferta de servicios financieros (B2C)	Las <i>FinTech</i> B2C análisis práctico y jurídico
Mundial	Organismo y Academia	World Bank and Cambridge Centre for Alternative Finance (CCAF)	2020	Todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros	Innovación	Sí	Oferta de servicios financieros (B2C)	<i>The Global Covid-19 FinTech Regulatory Rapid Assessment Study</i>
España	Asociación	(AEFI) Asociación Española de <i>FinTech</i> e <i>InsurTech</i>	2021		Innovación	No	Oferta de servicios financieros (B2C)	Libro blanco de la regulación <i>FinTech</i> en España

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
Europa	Autoridad	Comisión Europea	2018	La innovación en los servicios financieros posibilitada por la tecnología	Innovación	No	Oferta de servicios financieros (B2C)	Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador
Chile	Autoridad	Banco Central de Chile: Pablo Furche, Carlos Madeira, Mario Marcel, Carlos A. Medel	2017	Desarrollos financieros facilitados por la tecnología	Innovación	No	Amplio	<i>FinTech</i> y la banca central en la encrucijada
Global	Organismo	(IMF) International Monetary Fund	2018	<i>Advances in technology that have the potential to transform the provision of financial services spurring the development of new business models, applications, processes, and products</i> (Avances en tecnología que tienen el potencial de transformar la provisión de servicios financieros impulsando el desarrollo de nuevos modelos de negocios, aplicaciones, procesos y productos)	Innovación	Sí	Amplio	<i>IMF policy paper. The Bali FinTech Agenda</i>
Estados Unidos de América	Academia	McAuley, D.	2015	<i>An economic industry composed of companies that use technology to make financial systems more efficient</i> (Una industria económica compuesta por empresas que utilizan la tecnología para hacer más eficientes los sistemas financieros)	Entidad	No	Amplio	<i>What is FinTech?</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
Global	Organismo	FSB (Financial Stability Board)	2021	<i>Technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services</i> (Innovación tecnológicamente habilitada en servicios financieros que podría resultar en nuevos modelos comerciales, aplicaciones, procesos o productos con un efecto material asociado en los mercados e instituciones financieras y la provisión de servicios financieros)	Innovación	Sí	Amplio	<i>Financial innovation structural change. FinTech</i>
Global	Organismo	(IOSCO) International Organization of Securities Commissions	2017	<i>A variety of innovative business models and emerging technologies that have the potential to transform the financial services industry.</i> (Una variedad de modelos comerciales innovadores y tecnologías emergentes que tienen el potencial de transformar la industria de servicios financieros)	Innovación	Sí	Amplio	<i>IOSCO Research Report on Financial Technologies (FinTech)</i>
Global	Organismo	(BIS) Bank of International Settlements	2021	<i>FinTech refers to technology-enabled innovation in financial services</i> (FinTech se refiere a la innovación habilitada por la tecnología en los servicios financieros)	Innovación	No	Oferta de servicios financieros (B2C)	<i>Trending topics. Innovation and FinTech</i>
España	Autoridad	Banco de España: Jara Quintanero, Román Santos, Ana	2020	Un nuevo tipo de entidad, en contraposición a la banca tradicional, que ofrece servicios financieros	Entidad	No	Oferta de servicios	<i>FinTech: panorama y retos en la obtención de información</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
España	Autoridad	Fernández y Auxi Moreno (CNMV) Comisión Nacional del Mercado de Valores	Sin fecha	innovadores utilizando las tecnologías más modernas Todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros	Innovación	No	financieros (B2C) Oferta de servicios financieros (B2C)	¿Qué es <i>FinTech</i> ? Guía rápida
España	Organismo	(AEB) Asociación Española de Banca	2017	Innovación tecnológica aplicada a los servicios financieros, con independencia de la naturaleza o tamaño de la empresa que los presta	Innovación	No	Oferta de servicios financieros (B2C)	La innovación tecnológica aplicada a los servicios financieros está generando nuevos servicios y modelos de negocio ofrecidos tanto por los bancos tradicionales como por importantes empresas tecnológicas y nuevos entrantes
Global	Organismo	(FATF) Financial Action Task Force	2021	<i>FinTech refers broadly to the use of new and emerging digital technologies in the financial sector for any of a wide variety of purposes. Initially, "FinTech" primarily referred to the application of technology-based innovations to provide new customer-facing financial products and services [e.g., mobile payment solutions, on-line marketplace lending, algorithmic savings and investment tools, virtual currency payments, capital raising</i>	Innovación	No	Oferta de servicios financieros (B2C) y servicios de back office (B2B o infraestructura)	<i>Opportunities and challenges of new technologies for AML/CFT</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
				<p><i>(crowd funding) and deposit taking (remote check capture, mobile banking)]. FinTech now also encompasses the use of new and emerging technologies to provide automated mid- and back-office enterprise functions, such as the use of algorithms, big data, AI and machine learning, and link analytics for wholesale clearance, settlement, and other wholesale intermediation for e.g., securities, derivatives, wholesale finance, and payments, as well as regulatory compliance activities (see RegTech definition, below). Other applications remain to be developed. (FinTech se refiere ampliamente al uso de tecnologías digitales nuevas y emergentes en el sector financiero para cualquiera de una amplia variedad de propósitos. Inicialmente, "FinTech" se refería principalmente a la aplicación de innovaciones basadas en la tecnología para proporcionar nuevos productos y servicios financieros orientados al cliente [por ejemplo, soluciones de pago móvil, préstamos en el mercado en línea, herramientas algorítmicas de ahorro e inversión, pagos en moneda virtual, obtención de capital financiación) y captación de</i></p>				



País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
				depósitos (captura remota de cheques, banca móvil)]. <i>FinTech</i> ahora también abarca el uso de tecnologías nuevas y emergentes para proporcionar funciones empresariales automatizadas de <i>mid-office</i> y <i>back-office</i> , como el uso de algoritmos, big data, inteligencia artificial y aprendizaje automático, y análisis de enlaces para autorización mayorista, liquidación y otros mayoristas. intermediación para, por ejemplo, valores, derivados, financiación mayorista y pagos, así como actividades de cumplimiento normativo (consulte la definición de <i>RegTech</i> , a continuación). Quedan otras aplicaciones por desarrollar)				
América Latina	Organismo	Banco de Desarrollo de América Latina-CAF	2021	<i>Start-ups</i> especializadas en el diseño y desarrollo de productos y servicios financieros 100 % digitales	Entidad	No	Oferta de servicios financieros (B2C)	Diplomado en inclusión financiera. Módulo <i>FinTech</i> . Complemento a la información del gráfico
Alemania	Academia	Gimpel, H., D. Rau, and M. Röglinger	2018	<i>FinTech characterizes the usage of digital technologies such as the Internet, mobile computing, and data analytics to enable, innovate, or disrupt financial services. FinTech start-ups are newly established businesses that offer financial services based on FinTech. (FinTech caracteriza el uso de</i>	Innovación y entidad	Sí	Amplio	<i>Understanding FinTech start-ups – a taxonomy of consumer-oriented service offerings</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
México	Autoridad	(CNBV) Comisión Nacional Bancaria y de Valores	2018	<p>tecnologías digitales como internet, computación móvil y análisis de datos para habilitar, innovar o interrumpir los servicios financieros.</p> <p>Las <i>start-ups FinTech</i> son empresas de nueva creación que ofrecen servicios financieros basados en <i>FinTech</i>.)</p> <p>Instituciones de tecnología financiera reguladas en esta Ley, las cuales son las instituciones de financiamiento colectivo y las instituciones de fondos de pago electrónico</p>	Entidad	No	Oferta de servicios financieros (B2C)	Ley para regular las instituciones de tecnología financiera
Hong Kong	Academia	Arner, Barberis, Buckley, RP	DW; JN; 2015	<p><i>The use of technology to deliver financial solutions</i> (El uso de la tecnología para ofrecer soluciones financieras)</p> <p><i>There is still no clear definition of the concept of a FinTech company. Combining the words "financial services" and "technology", FinTech companies are commonly understood to be young undertakings that provide specialised and in particular customer-oriented financial services using technology-based systems</i> (Todavía no hay una definición clara del concepto de empresa <i>FinTech</i>. Combinando las palabras "servicios financieros" y "tecnología", las empresas <i>FinTech</i> se entienden comúnmente como empresas jóvenes que brindan servicios</p>	Innovación	No	Oferta de servicios financieros (B2C)	<i>The Evolution of FinTech: A New Post-Crisis Paradigm?</i>
Alemania	Autoridad	(BaFin) Financial Supervisory Authority	Federal 2021	<p><i>There is still no clear definition of the concept of a FinTech company. Combining the words "financial services" and "technology", FinTech companies are commonly understood to be young undertakings that provide specialised and in particular customer-oriented financial services using technology-based systems</i> (Todavía no hay una definición clara del concepto de empresa <i>FinTech</i>. Combinando las palabras "servicios financieros" y "tecnología", las empresas <i>FinTech</i> se entienden comúnmente como empresas jóvenes que brindan servicios</p>	Entidad	No	Oferta de servicios financieros (B2C)	<i>Company start-ups and FinTech companies</i>

País	Origen	Autor	Año	Definición	Orientación	Referencia a disrupción, materialidad, impacto o relevancia	Enfoque	Título
Reino Unido	Autoridad	Bank of England	2021	financieros especializados y, en particular, orientados al cliente utilizando sistemas basados en la tecnología.) <i>Technology-enabled financial innovation, which is changing the way financial institutions provide – and consumers and businesses use – financial services</i> (Innovación financiera habilitada por la tecnología, que está cambiando la forma en que las instituciones financieras brindan, y los consumidores y las empresas utilizan, los servicios financieros)	Innovación	No	Amplio	<i>Research. FinTech</i>

Anexo I. *Definiciones de FinTech*

Nota. Elaboración propia.



### ANEXO III. ETAPAS *FINTECH* Y SUS CARACTERÍSTICAS

<b>Etapa</b>	<b><i>FinTech 1.0</i></b>	<b><i>FinTech 2.0</i></b>	<b><i>FinTech 3.0 a 3.5</i></b>		<b><i>FinTech 4.0</i></b>
<b>Subetapa</b>	N.A.	N.A.	<i>FinTech 3.0</i>	<i>FinTech 3.5</i>	N.A.
<b>Fechas</b>	1866-1967	1967-2008	2008-2020		2020-actualidad
<b>Circunstancias históricas</b>	1866- Primer mensaje telegráfico transatlántico 1914-1918- Primera Guerra Mundial 1929- Caída de la bolsa de Nueva York 1030- Gran Depresión 1939-1945- Segunda Guerra Mundial	1975- Comité de Basilea 1980- Crisis de la deuda en América Latina 1986- <i>Single European Act</i> 1987- Lunes Negro 1988- Basilea I 1990- <i>Bank of International Settlements Payments and Settlement Committee</i> 1992- Tratado de Maastricht (Unión Europea) 1998 - Banco Central Europeo (ECB) 1999- TARGET 2000- <i>E-money directive</i> 2002- Introducción de monedas y billetes Euro 2004- Basilea II Nov 2007- Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET 2) Dic 2007- Directiva de Servicios de Pago (PSD I)	2008-2009 Crisis financiera global 2008 - Publicación de artículo sobre Bitcoin 2008 - Implantación de Basilea II 2009 – Directiva Entidades Emisoras de Dinero Electrónico (EMI) 2010 - <i>Dodd Frank Act</i> 2010 - Basilea III 2011- Autoridad Bancaria Europea (EBA) 2014 - Ethereum y uso de <i>smart contracts</i> 2015- Segunda directiva de servicios de pago (implantación de <i>Open Banking</i> en Europa) 2016 - <i>BIS Payments and Market Infrastructure Committee</i>		2023- Reglamento <i>Markets in Cryptoassets</i> (MiCA) 2021- Explosión de <i>tokens</i> no fungibles (NFT). 2021- Desarrollo del Metaverso y la Web 3.0 2021- Bitcoin como moneda de curso legal en El Salvador 2021- Proyecto de Euro Digital
<b>Geografía</b>	Global	Global	Global	Global	Global
<b>Primeras adopciones (liderazgo)</b>	Países desarrollados	Países desarrollados	Países desarrollados	Países emergentes	Países emergentes

Etapa	FinTech 1.0	FinTech 2.0	FinTech 3.0 a 3.5		FinTech 4.0
<b>Proveedores de servicios financieros</b>	Banca tradicional	Banca tradicional	Banca FinTech/ Banca Tradicional	100 % Digital BigTech	DAO (Organizaciones autónomas descentralizadas) Banca FinTech/ Banca Tradicional
<b>Evolución de finanzas centralizadas a finanzas descentralizadas</b>	CeFi -Centralizadas (tercero de confianza)	CeFi -Centralizadas (tercero de confianza)	CeDeFi- Descentralización centralizada (el tercero de confianza cambia, pero sigue existiendo una entidad jurídica a cargo de la operativa)		DeFi – Descentralizadas, no tiene por qué existir una entidad jurídica. La tecnología reemplaza al tercero de confianza
<b>Concepto de banca</b>	Banca cerrada	Banca cerrada	Banca abierta (vertical de pagos)		Finanzas abiertas (todos los verticales)
<b>Nivel de impacto de las innovaciones</b>	Evolución	Evolución	Disrupción		Disrupción
<b>Modelo supervisor europeo</b>	Tradicional	Tradicional	Aparición de <i>SupTech</i> y <i>Sandbox</i>		Aún por determinar
<b>Público beneficiado</b>	Bancarizado	Bancarizado	Bancarizado y sub bancarizado		No bancarizado y sub bancarizado
<b>Filtros para acceder al producto o servicio</b>	Alto	Alto	Medio		Bajo
<b>Infraestructura operativa</b>	Tradicional	Tradicional	Tradicional con elementos de mejora (en lo fundamental, aún opera sobre infraestructura heredada de banca tradicional)		Infraestructuras alternativas no basados en esquemas heredados
<b>Características</b>	Foco en <i>hardware</i> Primeros ordenadores	Banca telefónica Internet (web)	Reducción de barreras a los servicios financieros digitales Aparición de nuevos agentes ( <i>FinTech, TechFin</i> ) Finanzas móviles (smartphone) Nuevos modelos de negocio Servicios <i>peer to</i>	Reducción de barreras a los servicios financieros digitales Aparición de nuevos agentes ( <i>FinTech, TechFin</i> ) Foco en la explotación de datos: Analítica de datos, <i>big data</i> Concentración de innovaciones aplicadas a finanzas Finanzas móviles	Democratización de los servicios financieros digitales Usuarios recuperan la hegemonía sobre todos sus datos financieros ( <i>Open Finance</i> ) Finanzas descentralizadas - eliminación de terceros de intermediarios tradicionales Drástica reducción de costes, optimización de tiempos de operativos Países emergentes como <i>early</i>

<b>Etapa</b>	<b>FinTech 1.0</b>	<b>FinTech 2.0</b>	<b>FinTech 3.0 a 3.5</b>		<b>FinTech 4.0</b>
			<i>peer</i> (pagos, financiación) Usuarios con control sobre datos relacionados con pagos ( <i>Open Banking</i> )	( <i>smartphone</i> ) Servicios <i>peer to peer</i> (pagos, financiación) Nuevos modelos de negocio Usuarios con control sobre datos relacionados con pagos ( <i>Open Banking</i> ) Países emergentes como <i>early adopters</i> de criptoactivos	<i>adopters</i> de servicios de criptoactivos
<b>Principales innovaciones empleadas en finanzas</b>	Telégrafo	Cajero automático (ATM) Desarrollo de SWIFT ( <i>Society for Worldwide Interbank Financial Telecommunication</i> )	<i>Smartphone</i> <i>Application Programming interface</i> (API) Analítica de datos <i>Machine learning</i> e inteligencia artificial		Tecnología de registros distribuidos (DLT)
<b>Desencadenantes exógenos</b>	Posindustrialización y posguerra: interconexión de países. Globalización.	Digitalización Comercio electrónico Teléfono móvil	Crisis financiera Aparición de <i>smartphones</i>	Estrategias políticas digitales (países asiáticos y América Latina)	Crisis COVID-19 Web 3.0

Tabla 13. *Etapas de los avances FinTech*

Nota. Elaboración propia





## ANEXO IV. PUBLICACIONES

El trabajo de investigación desarrollado durante esta tesis ha brindado la posibilidad de publicación de algunos artículos y capítulos de libro en el entorno académico-jurídico, cuyo detalle puede verse a continuación:

### Artículos:

- Castro, Á., & Suárez, L. (2021). Oferta de servicios de criptoactivos por parte de entidades del sistema financiero: análisis comparativo entre Perú y la Unión Europea. *Revista de Estudiantes Ita Ius Esto*, 19-19. Perú.
- Suárez, L. (2021). Instrumentos administrativos para el fomento de la innovación tecnológica en el sector financiero peruano. *Derecho PUCP*, (87), 183-229. Perú.
- Suárez, L. (2022). La problemática de emisión de *tokens* y plataformas de negociación de los mismos bajo la perspectiva del *case law* estadounidense. *Revista de derecho del mercado de valores*, (30), 5. España.
- Suárez, L. (2023). *FinTech* and financial inclusion: analysis from a financial dignity approach. *Estudios Socio-Jurídicos*, 25(2). Colombia.
- Suárez, L. (2023) Decentralized Finance Oracles, *Journal of New Finance: Vol. 3: No. 1, Article 2*. DOI: 10.46671/2521-2486.1016. España.

### Capítulos de libro:

- Suárez, L. (2021). Retos jurídicos de las estrategias de incursión de las plataformas de la *gig economy* de movilidad (*ride hailing*) en el mundo financiero modelos de negocios en entornos de pagos digitales. En *Plataformas digitales: aspectos jurídicos* (pp. 285-303). Aranzadi. España.
- Suárez, L. (2022). Central Bank Digital Currencies (CBDC): Reacciones de los bancos centrales ante la expansión del uso de criptomonedas y sus implicaciones jurídico-económicas. En Parra, C., *Derecho digital y nuevas tecnologías* (pp. 937-956). Aranzadi. (pp. 937-956). Aranzadi. España.



## ÍNDICES



## ÍNDICE DE TABLAS

<i>Tabla 1. Resultados de búsqueda con la palabra “FinTech” en las bases de datos de Dialnet y Scopus a 14 de febrero de 2022.....</i>	<i>32</i>
<i>Tabla 2. Análisis comparativo FinTech start-up, TechFin y entidades financieras.....</i>	<i>81</i>
<i>Tabla 3. Análisis comparativo de servicios en banca y finanzas abiertas.....</i>	<i>120</i>
<i>Tabla 4. Visión general de los potenciales riesgos de las finanzas abiertas.....</i>	<i>123</i>
<i>Tabla 5. Iniciativas de banca y finanzas abiertas por país/región a diciembre de 2021.....</i>	<i>124</i>
<i>Tabla 6. Ejemplos del potencial de las nuevas tecnologías en el sector asegurador.....</i>	<i>167</i>
<i>Tabla 7. Ejemplos de innovaciones y su uso en RegTech (sector privado y público).....</i>	<i>174</i>
<i>Tabla 8. Origen de conceptos aplicados en Blockchain y Bitcoin.....</i>	<i>203</i>
<i>Tabla 9. Ejemplo de dimensiones para tener en cuenta para catalogar un token.....</i>	<i>208</i>
<i>Tabla 10. Ejemplos de actividades en roles tradicionales y su equivalente en las finanzas descentralizadas.....</i>	<i>221</i>
<i>Tabla 11. Análisis de Dex y AMM y su operativa en distintas Blockchain a 24 de diciembre de 2021 ...</i>	<i>283</i>
<i>Table 12 FinTech action plan overview and status as of July 2022.....</i>	<i>373</i>
<i>Table 13 Overview of priorities under the 2020 EU Digital Finance Strategy, with detail of the action plans and areas impacted.....</i>	<i>374</i>
<i>Table 14 Overview of the existing token main European regulatory framework (excluding transversal financial regulations such as financial crime (Directive (EU) 2015/849 ), tax or consumer protection related).....</i>	<i>382</i>
<i>Table 15 Obligations of regulated agents under DMA.....</i>	<i>432</i>



## ÍNDICE DE FIGURAS

Figura 1. Evolución estimada de la capacidad tecnológica en 20 años .....	34
Figura 2. Ejemplos de disrupciones tecnológicas en el sector financiero .....	40
Figura 3. Agentes en la industria financiera actual. Estrategias de origen y evolución en función de su tamaño y foco .....	49
Figura 4. Capitalización de BigTech versus los mayores grupos financieros .....	77
Figura 5. Futuros modelos de negocio de la banca .....	80
Figura 6. Pirámide de necesidades económicas .....	86
Figura 7. Comparativa de flujos en procesos de pagos antes y después de PSD II.....	92
Figura 8. Flujo operativo de iniciadores de pagos bajo PSD II .....	93
Figura 9. Flujo operativo de agregadores de pagos bajo PSD II.....	94
Figura 10. Comparativa Marketplace Banking con Embedded Finance .....	97
Figura 11. Ejemplo de relaciones de corresponsalía para una operación en dólares entre un ordenante en España y un beneficiario en México.....	104
Figura 12. Modelo de transferencias entre dos países de zona SEPA con bancos miembros indirectos de las cámaras de compensación y liquidación .....	106
Figura 13. Evolución de la banca abierta: del inicio al más allá.....	119
Figura 14. Ejemplo de oferta de servicios BigTech .....	134
Figura 15. Ejemplo de dependencias y relaciones entre proveedores de servicios de computación en la nube, BigTech regionales y entidades financieras sistémicas .....	135
Figura 16. Ecosistema FinTech 3.0-3.5 .....	137
Figura 17. Comparativa de crecimiento interanual en servicios de financiación. La concesión de hipotecas se ha disparado .....	141
Figura 18. Árbol de decisión de los modelos de crowdfunding en función del tiempo que se mantiene la relación con las contrapartes.....	148
Figura 19. Ejemplo de esquema comparativo de la operativa de financiación en banca tradicional frente a crowdlending .....	154
Figura 20. FCA Data & Analytics Hub: modelo operativo del hub y las distintas unidades de data science .....	172
Figura 21. Espectro de riesgos RegTech y niveles de priorización.....	173
Figura 22. Ejemplo de modelo de integración de una FinTech (Marketplace) en BaaS en el que las operaciones financieras son secundarias o complementarias de las principales .....	178
Figura 23. Ejemplo de plataformas operadas por BigTech en las que existe intercambio de información y de transacciones (financieras y no financieras) a través de la plataforma.....	178
Figura 24. Ejemplo comparativo de los modelos operacionales previos a la implementación de normativas de API abiertas y posteriores a esta .....	182
Figura 25. Ejemplo de infraestructura tecnológica en modelo Banking as a Service de un neobanco .....	185
Figura 26. Ejemplo de infraestructura modular en el FinTech as a Service de pagos .....	186
Figura 27. Operativa con claves criptográficas públicas y privadas .....	203
Figura 28. Ejemplos de asignación de tokens y su distribución a octubre de 2020.....	212
Figura 29. Gráfico de relación de modelos societarios y nuevas tecnologías .....	217
Figura 30. Infraestructura modelo del ecosistema de finanzas descentralizadas (DeFi) y su interoperabilidad con otros ecosistemas .....	227
Figura 31. Triángulo de las stablecoins.....	234
Figura 32. Visión funcional de un ecosistema stablecoin. Ejemplos seleccionados .....	235
Figura 33. Taxonomía de tokens no fungibles (NFT).....	253
Figura 34. Comparativa de costos en los esquemas tradicionales de pago en comercio frente a hipotéticos esquemas de pago DeFi.....	269
Figura 35. Comparativa de los esquemas tradicionales de crédito frente a esquemas DeFi .....	271
Figura 36. Esquema de operativa en Security Token Offering (STO).....	275
Figura 37. Comparativa de los esquemas tradicionales de cambio de divisas frente a esquemas DeFi .....	280
Figura 38. Esquema operativo de Automated Money Market Makers (AMM) en finanzas descentralizadas (alto nivel) .....	281
Figura 39. Comparativa de los esquemas tradicionales de gestión de activos frente a esquemas DeFi .....	284
Figura 40. Esquema operativo de servicios de custodia tradicionales .....	289

<i>Figura 41. Comparativa de los esquemas tradicionales de seguros frente a esquemas DeFi .....</i>	<i>294</i>
<i>Figura 42. Ejemplo de la operativa de un oráculo.....</i>	<i>297</i>
<i>Figura 43. Volumen de transacciones por categoría de tamaño de transferencia, junio de 2021 a mayo de 2022, Algorand, Bitcoin y Ethereum .....</i>	<i>300</i>
<i>Figura 44. Capas de supervisión por verticales de la industria financiera .....</i>	<i>315</i>
<i>Figura 45. Estructura organizacional del JCESA y su involucración en asuntos de innovación de acuerdo con su plan de trabajo para 2022.....</i>	<i>317</i>
<i>Figura 46. Flujos operativos en el Single Supervision Mechanism (Mecanismo Único de Supervisión) .....</i>	<i>319</i>
<i>Figura 47. Ciclo de vida de innovación, regulación y supervisión en las etapas FinTech 1.0 y 2.0 .....</i>	<i>325</i>
<i>Figura 48. Ciclo de vida de innovación, regulación y supervisión en las etapas FinTech 3.0 y 3.5 .....</i>	<i>326</i>
<i>Figura 49. Ciclo de vida de innovación, regulación y supervisión en la etapa FinTech 4.0 .....</i>	<i>327</i>
<i>Figura 50. Metodología PDCA aplicada a los procesos de producción normativa FinTech .....</i>	<i>340</i>
<i>Figura 51. Diagrama de Venn de las actividades reguladas frente a actividades FinTech.....</i>	<i>352</i>
<i>Figura 52. Diagrama de Venn de riesgos regulados frente a riesgos FinTech.....</i>	<i>354</i>
<i>Figura 53. Diagrama de Venn de la aplicación analógica del principio de misma actividad, mismo riesgo, misma norma. ....</i>	<i>356</i>
<i>Figura 54. Propuesta del modelo regulatorio FinTech.....</i>	<i>358</i>
<i>Figura 55. Propuesta del modelo de supervisión delegada .....</i>	<i>362</i>
<i>Figure 56 Comparative of traditional Operational scheme versus optimized scheme under DLT Pilot Regulation .....</i>	<i>407</i>
<i>Figure 57 Schematic diagram of the SSI workflow .....</i>	<i>441</i>



## **REFERENCIAS**



## REFERENCIAS

### Bibliografía – libros y capítulos de libros

- Alonso, C. (2021). Presentación del libro "Tokens-valor (Security Tokens). Régimen de los criptoactivos negociales y sus mercados (MiCAs)" Reus ed., Madrid (2021). In J. I. Jiménez (Eds.), *Token Law and Markets* (pp. 69-77). Editorial Reus.
- Alonso, C., Muñoz, A.F., Aragón, I., Fernández, I., Gullón, P., Prieto, L., & Ruiz, F. (2020). *Memento Práctico de Mercados Financieros 2020-2021. Banca, Bolsa y Seguros*. Lefebvre-El Derecho S.A.
- Alvarado, L. (2021). Autorización de los proveedores de servicios de criptoactivos. In Madrid, A. y Pastor, C. (Eds.), *Guía de criptoactivos MiCA* (pp. 245-259). Thomson Reuters Aranzadi.
- Anderson, A. (2019). *Stablecoins for beginners*. Independently published.
- Annunziata, F. (2021). Innovaciones en el marco de los proveedpres de servicios de pago. Perspectiva europea. En M. Cuenca , & J. Ibáñez, *Perspectiva legal y económica del fenómeno FinTech* (pp. 293-308). Wolters Kluwer Legal & Regulatory España, S.A.
- Barrio M., & Muñoz, A.F. (2021). *Criptoactivos. Retos y desafíos normativos*. Wolters Kluwer España, S.A.
- Barrio, M. (2021). La revolución "FinTech". Definición, factores desencadenantes, oportunidades y riesgos. En M. Cuenca Casas, & J. Ibáñez Jiménez (Eds.), *Perspectiva legal y económica del fenómeno FinTech* (pp. 59-67). Wolters Kluwer.
- Barrio, M. (2020). *Manual de derecho digital*. Tirant lo blanch.
- Benson, C. C. (2020). *Global Payments and the FinTech Innovations Changing de Industry*. Glenbrook.
- Bobbio, N. (2016). *Teoría general del derecho*. Temis.
- Brummer, C. (2020). *FinTech Law in a nutshell*. LEC, Inc. d/b/a West Academic.
- Caballero, M. (2019). *Bitcoin. Blockchain y tokenización para inquietos*. Bubock Editorial.
- Caballero, M., Ramió, A., & Carrera, M. (2020). *Finanzas descentralizadas para inquietos*. Bubok Editorial.
- Camacho, S. (2018). Las modalidades de financiación participativa o crowdfunding y su distinción respecto a figuras afines: equity-crowdfunding emisión de valores y obligaciones, crowdlending y mecenazgo participativo. En A. Martínez-Echevarría, &

- F. Pañeda Usunáriz, *Las plataformas de financiación participativa-crowdfunding* (pp. 31-48). Thomson Reuters Aranzadi.
- Campbell, R. H., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance*. John Wiley & Sons.
- Ciraolo, F. (2022). Payment tokens y la legislación europea sobre servicios de pago. En C. P. Sempere, *Dinero digital y gobernanza TIC en la Unión Europea* (pp.91-114). Thomson Reuters Aranzadi.
- Cuena, M. (2019). *Las FinTech de préstamos o crowdlending. La contratación a través de plataformas intermediarias en línea*. REUS, S.A.
- Cuena, M. (2022). *Contratación a través de plataformas de financiación participativa contenida en Ley 5/2015 de fomento de financiación empresarial a la luz del Reglamento 2020/1503/UE*. Universidad Complutense de Madrid.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law*. Harvard University Press.
- Dragomir, L. (2010). *European Prudential Banking Regulation and Supervision. The legal dimension*. Routledge Research in Finance and Banking Law.
- Engisch, K. (1967). *Introducción al pensamiento jurídico*. <https://teoriageneralalderecho122014.files.wordpress.com/2011/06/engisch-karl-introduccion-al-pensamiento-juridico.pdf>
- García, G. (2007). *Cien años de soledad*. Ediciones Cátedra.
- García, P. (2018). Del ciberderecho al criptoderecho. La criptoregulación. En P. García Mexía, *Criptoderecho. La regulación de Blockchain* (pp.75-140). Wolters Kluwer España, S.A.
- González de Audinaca, F. (2019). *Las FinTech B2C análisis práctico y jurídico*. Aferre Editor S.L.
- Guaita, J. M., Carracedo, P., & Isidro, F. (2019). *Las criptomonedas: Digitalización del dinero 2.0*. Thomson Reuters Aranzadi.
- Hagenfeldt, V. (2009). *European financial regulation and supervision on the onslaught of the financial crisis*. GIN Verlag.
- Ibañez, J. (2021). MiCA Regulation: legal matters still pending. En Ibañez, J. (Eds.), *Token law and markets* (pp. 25-39). Editorial Reus.
- Kuhn, T. (1962). *The Structure of Scientific Revolutions*. University of Chicago Press.
- Liker, J. K. (2006). *Las claves del éxito de Toyota*. Centrol Libros PAPP, S.L.U.

- Martinero, J. (2022). NFTs (Non-fungible tokens) y el metaverso. En E. Ortega Burgos, *Nuevas Tecnologías 2022* (pp.329-340). Tirant lo blanch.
- Martínez, A. (2021). Ámbito de aplicación y conceptos esenciales de la propuesta de Reglamento relativo a los mercados de criptoactivos: la noción de criptoactivo y sus subcategorías (arts. 2 y 3). En Madrid, A. y Pastor, C., *Guía de criptoactivos MiCA* (pp.41-62). Aranzadi S.A.U.
- Maslow, A. H. (1954). *Motivation and personality*. [http://s-f-walker.org.uk/pubsebooks/pdfs/Motivation\\_and\\_Personality-Maslow.pdf](http://s-f-walker.org.uk/pubsebooks/pdfs/Motivation_and_Personality-Maslow.pdf)
- McKinney, E. (2020). *The DeFi Revolution*. Independently published.
- Morales, J. (2018). ¿Qué es blockchain? En P. García Mexía, *Criptoderecho. La regulación de Blockchain*. Wolters Kluwer España, S.A.
- Ortega, A. (2019). *"Smart Contracts" y derecho internacional privado*. Thomson Reuters (Legal) Limited.
- Ortiz, M. L. (2018). *La supervisión bancaria europea. Régimen jurídico*. Mc Graw Hill Education.
- Otero, M. (2021). Régimen de información y transparencia: El libro blanco de criptoactivos. En Madrid, A. y Pastor, C., *Guía de criptoactivos MiCA* (pp.189-204). Navarra: Thomson Reuters Aranzadi.
- Paracampo, M. (2022). Los proveedores de servicios de criptoactivos entre antiguos y nuevos players. En C. Pastor Sempere, *Dinero Digital y Gobernanza TIC en la UE* (pp.149-172). Editorial Aranzadi S.A.U.: Navarra.
- Paredes, A. (2018). Aproximaciones al crowdfunding. En A. Martínez-Echevarría, & F. Pañeda Usunáriz, *Las plataformas de financiación participativa-crowdfunding*. Thomson Reuters Aranzadi.
- Peñas, M. (2020). Régimen jurídico de los servicios de pago en el Derecho Español. *Thomson Reuters Aranzadi*. <https://www.thomsonreuters.es/es/tienda/duo-papel-ebook/regimen-juridico-de-los-servicios-de-pago-en-el-derecho-espanol.-mono-grafia-revista-de-derecho-del-sistema-financiero-num.-1-2020duo/p/10016956>
- Petit, N. (2020). *Big Tech and the Digital Economy: the Monopoly Scenario*. Oxford University Press.
- Robles, G. (2015). *Teoría del derecho. Fundamentos de teoría comunicacional del derecho. Volumen II*. Thomson Reuters.
- Rodilla, M. (2014). *Teoría del Derecho*. Ratio Legis.

- Rodríguez de las Heras, T. (2019). *Challenges of FinTech to Financial Regulatory Strategies*. Marcial Pons Ediciones Jurídicas y Sociales S.A.
- Rodríguez, J. (2019). *FinTech* desde la perspectiva de la promoción de la competencia. En F. Zunzunegui, *Regulación Financiera y FinTech*. Editorial Aranzadi S.A.U.
- Sánchez, A. (2019). *Epistemología y metodología jurídica*. Tirant lo Blanch.
- Serrano, A. (2022). *Metaverso y derecho*. Tecnos.
- Smith, A. (1776). *La riqueza de las naciones*. Alianza Editorial.
- Suárez, L. (2022). Central Bank Digital Currencies (CBDC): Reacciones de los bancos centrales ante la expansión del uso de criptomonedas y sus implicaciones jurídico-económicas. En Parra, C., *Derecho digital y nuevas tecnologías* (pp.937-956). Aranzadi.
- Tanda, A., & Schena, C.-M. (2019). *FinTech, BigTech and Banks*. Palgrave Macmillan Studies in Banking and Financial Institutions.
- Tapia, A. (2020). *Guía de la contratación bancaria y financiera*. Thomson Reuters Aranzadi.
- Ugolini, S. (2017). *The evolution of central banking: theory and history*. Palgrave Studies in Economic History.
- V.V.A.A. (2021). *Criptoactivos. Retos y desafíos normativos*. Las Rozas (Madrid): Wolters Kluwer España, S.A. doi:978-84-186662-08-9
- Zunzunegui, F., Cuenca, M., Ribón, E., Rodríguez, J., Sola, F., & Tapia, A. (2019). *Regulación Financiera y FinTech*. Thomson Reuters Aranzadi.

## Bibliografía – artículos académicos

- Aguiló, J. (2021). Lagunas Constitucionales. *Anuario de Filosofía del Derecho*, (37), pp. 15-38. <https://doi.org/10.53054/afd.vi37.7733>
- Alvarado, L. (2017). El servicio de iniciación de pagos en la Directiva 2015/2366 sobre servicios de pago en el mercado interior. *La Ley Mercantil*, 10. <https://dialnet.unirioja.es/servlet/articulo?codigo=5894687>
- Antoneus, F., Broto, M., & Subanidja, S. (2021). *FinTech* as The Emerging Technologies in Banking Industry: Past, Present, and Future. *International Journal of Progressive Sciences and Technologies*, 28(2), pp. 371-378. <https://ijpsat.org/index.php/ijpsat/article/view/3550>.
- Apestequia, J., Oechssler, J., & Weidenholzer, S. (2019). *Copy trading*. *Economics Working Paper*. Economics Working Papers 1615, Department of Economics and Business, Universitat Pompeu Fabra, revised Sep 2019: <https://ideas.repec.org/p/upf/upfgen/1615.html>
- Arner, D. W. (2016). *FinTech: Evolution and Regulation*. [https://law.unimelb.edu.au/\\_\\_data/assets/pdf\\_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf](https://law.unimelb.edu.au/__data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf)
- Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of *FinTech*: A new post-crisis paradigm. *Geo. J. Int'l L.*, 47. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2676553](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676553)
- Awrey, D. (2021). Unbundling Banking, Money and Payments. *Law Working Paper N° 565/2021*.
- Barefoot, J. (2020). *Digitizing Financial Regulation: RegTech As A Solution for Regulatory Inefficiency and Ineffectiveness*. Mossavar-Rahmani Center for Business & Government or of Harvard University: [https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP\\_150\\_final.pdf](https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_150_final.pdf)
- Bech, M., & Garrat, R. (2017). *Central bank cryptocurrencies*. BIS Quarterly Review, Bank of International Settlements: [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.pdf](https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf)
- Bennett, N., & Lemoine, G. (2014). *What VUCA Really Means for You*. Harvard Business Review: <https://hbr.org/2014/01/what-vuca-really-means-for-you>

- Bethlendi, A., & Szócs, Á. (2022). How the *FinTech* ecosystem changes with the entry of Big Tech companies. *Investment Management and Financial Innovations*, 19(3), 38-48. [http://dx.doi.org/10.21511/imfi.19\(3\).2022.04](http://dx.doi.org/10.21511/imfi.19(3).2022.04)
- Cárdenas, E. R. (2021). ¿Por qué es importante regular el *FinTech*? *Revista de la Academia Colombiana de Jurisprudencia*, 1(373), 79-105. [https://revista.academiacolombianadejurisprudencia.com.co/index.php/revista\\_acj/article/view/189](https://revista.academiacolombianadejurisprudencia.com.co/index.php/revista_acj/article/view/189)
- Casey, M., & Vigna, P. (2018). *In blockchain we trust*. MIT Technology Review: <https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/>
- Castillo, A. (2020). Distributed Ledger Technology en el mercado de pagos: más allá de las criptomonedas. *Revista de Derecho del Mercado de Valores*, (27), 123-62. <https://dialnet.unirioja.es/servlet/articulo?codigo=7773367>
- Cong, L. W., Li, X., Tang, K., & Yang, Y. (2020). *Crypto Wash Trading*. <https://arxiv.org/abs/2108.10984>
- Cousaert, S., Xu, J., & Matsui, T. (2021). *SoK: Yield Aggregators in DeFi*. <https://arxiv.org/pdf/2105.13891.pdf>
- Dávila, J. (2019). Verdades y postreos sobre la identidad digital soberana. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, 28(135), 122-124.
- Fairfield, J. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*, 4(97), 1261-1314. <https://www.repository.law.indiana.edu/ilj/vol97/iss4/4/>
- Frost, J., Gambacorta, L., Huang, Y., Song Shin, H., & Zbinden, P. (2019). *BigTech and the changing structure of financial intermediation*. Bank of International Settlements [BIS]; Monetary and Economic Department.
- Geczy, C. (2021). *Application of AI, InsurTech and Real Estate Technology. Introduction to InsurTech*. Wharton University of Pennsylvania.
- Gorjón, S. (2022). *Las grandes tecnológicas y los servicios financieros: algunos desafíos, beneficios y respuestas regulatorias*. <https://repositorio.bde.es/bitstream/123456789/19211/1/be2104-art39.pdf>
- Haber, S., & Stornetta, W. (1990). How to time-stamp a digital document. *Conference on the Theory and Application of Cryptography* (pp.437-455). Springer.



- Jensen, J., von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*, 26, 46-54. doi:<https://doi.org/10.7250/csimq.2021-26.03>
- Kaleem, M., & Shi, W. (2021). *Demystifying Pythia: A Survey of ChainLink. Oracles Usage on Ethereum*. *arXiv:2101.06781v2*. <https://arxiv.org/pdf/2101.06781.pdf>
- Lambert, T., Roosenbo, P., & Libeau, D. (2020). *Security token offerings*. Small Business Economics.
- Long, C. (2021). Ten Stablecoin Predictions and their Monetary Policy Implications. *Cato Journal*, 41(2), 307-319. 10.36009/CJ.41.2.9
- Macagno, F., & Walton, D. (2009). Argument from analogy in Law, the Classical Tradition, and Recent Theories. *Philosophy and Rhetoric*, 42(2), 154-182. 10.1353/par.0.0034
- Magalhães, P., & Ringe, W.-G. (2021). *Dynamism in Financial Market Regulation: Harnessing Regulatory and Supervisory Technologies*. Stanford Journal of Blockchain Law & Policy: <https://stanford-jblp.pubpub.org/pub/RegTech-SupTech-blockchain/release/1>
- Millar, C., Groth, O., & Mahon, J. (2018). Management innovation in VUCA world: challenges and recommendations. *California management review*, 61(1), 5-14. <https://doi.org/10.1177/0008125618805111>
- Mishra, S. (2009). *Virtual banking: from conventional to competitive approach*. NIIS Institute of Business Administration: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1842923](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1842923)
- Moreno, M. (2021). La certeza y simbolización de los derechos subjetivos: Tokens y contratos inteligentes. *Revista de Derecho, Empresa y Sociedad (REDS)*, (18), 57-72. <https://dialnet.unirioja.es/servlet/articulo?codigo=8359984>
- Mueller, J. (2018). *InsurTech Rising: A Profile of the InsurTech Landscape*. Milken Institute, 10.
- Müller, S., & Tworek, H. (2015). The telegraph and the bank': on the interdependence of global communications and capitalism, 1866–1914. *Journal of Global History*, 10(2), 259-283. <https://doi.org/10.1017/S1740022815000066>.
- Muñoz, A.F. (2017). «Criptomonedas», el «dinero mágico». Aspectos jurídicos. *Revista de Derecho del Mercado de Valores*, (21), 1-13. <https://dialnet.unirioja.es/servlet/articulo?codigo=6265717>

- Muñoz, A.F. (2018). Crowdfunding en Europa; entre la fragmentación y la unidad de mercado. *Revista de Derecho del Mercado de Valores*, (22), 1-18. <https://dialnet.unirioja.es/servlet/articulo?codigo=6517186>
- Murphy, D., & Mueller, J. (2018). *RegTech: Opportunities for More Efficient and Effective Regulatory Supervision and Compliance*. Milken Institute, Vol. 11
- Navarro, G. (2019). Aplicación de la tecnología blockchain a emisiones de valores negociables. *Revista privacidad y derecho digital*, 4(15), 127-170. <https://dialnet.unirioja.es/servlet/articulo?codigo=7210811>
- Navarro, G. (2021). Trading and settlement in crypto-assets. *Revista de Privacidad y Derecho digital*, 65-98. <https://dialnet.unirioja.es/servlet/articulo?codigo=7899934>
- Padilla, J. (2020). *BigTech “banks”, financial stability and regulation*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3580888](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3580888)
- Pascual, A. P. (2017). Identidad digital sobre «Blockchain» a nivel nacional. *ICADE. Revista de la Facultad de Derecho*, (101). <https://doi.org/10.14422/icade.i101.y2017.006>
- Pérez, C. (2022). Lagunas jurídicas y voluntad de derecho. *Diálogos Jurídicos*, 7, 293-312. <https://reunido.uniovi.es/index.php/dj/article/view/18591>
- Pérez, J. (2019). Una aproximación a las finanzas descentralizadas. *Papeles de Economía Española*, 141-177. [https://www.funcas.es/wp-content/uploads/Migracion/Articulos/FUNCAS\\_PEE/162art11.pdf](https://www.funcas.es/wp-content/uploads/Migracion/Articulos/FUNCAS_PEE/162art11.pdf)
- Perez, R. (2022). La nueva regulación europea de intermediarios digitales: Digital services act. *Información Comercial Española, ICE: Revista de economía*, (925), 41-51. <https://dialnet.unirioja.es/servlet/articulo?codigo=8433717>
- Priem, R. (2020). Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. *Financ Innov.*, 6(11). [:https://doi.org/10.1186/s40854-019-0169-6](https://doi.org/10.1186/s40854-019-0169-6)
- Qin, K., Zhou, L., & Afonin, Y. (2021). *CeFi vs. DeFi-Comparing Centralized to Decentralized Finance*. <https://arxiv.org/abs/2106.08157>
- Ramos, J. (2017). Lagunas del derecho y positivismo. Un examen de la concepción de las lagunas de C. Alchourrón y E. Bulygin. *Cuadernos de Filosofía del Derecho*, (40), 49-68. <https://doi.org/10.14198/DOXA2017.40.02>
- Rincón, E. (2021). ¿Por qué es importante regular el FinTech? *Revista de la Academia Colombiana de Jurisprudencia*, 1(373), 79-105.

[https://revista.academiacolombianadejurisprudencia.com.co/index.php/revista\\_acj/article/view/189](https://revista.academiacolombianadejurisprudencia.com.co/index.php/revista_acj/article/view/189)

Rodríguez de las Heras, T. (2013). El crowdfunding: una forma de financiación colectiva, colaborativa y participativa de proyectos. *Revista Pensar en Derecho*, 2(3). 101-123.

Rodríguez de las Heras, T. (2021). Las plataformas: nuevos actores (y reguladores) de la actividad económica. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 403-417.

Rodríguez, J. (1999). Lagunas axiológicas y relevancia normativa. *Doxa* 22, 349-369. <https://doi.org/10.14198/DOXA1999.22.16>

Salguero, M. (2017). Proporcionalidad y elaboración suareciana de la atribución intrínseca como fundamento filosófico de la analogía iuris y de la analogía legis. *Anales de la Cátedra Francisco Suárez*, 51. 101-128. <https://doi.org/10.30827/acfs.v51i0.6249>

Sandner, P., Gross, J., Grale, L., & Schulden, P. (2020). *The Digital Programmable Euro, Libra and CBDC: Implications for European Banks*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3663142](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3663142)

Schär, F. (2021). *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*. Economic Research Federal Reserve Bank of Saint Louis: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3571335](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335)

Schwarcz, S. L. (2021). Regulating Digital Currencies: Central Bank-Sponsored and Stablecoins. *Boston University Law Review* Vol 102:1037 (1038-1081). <https://www.bu.edu/bulawreview/files/2022/04/SCHWARCZ.pdf>

Segura, M. (1989). El problema de las lagunas en el derecho. *Anuario de filosofía del derecho*, VI, 285-312. <https://dialnet.unirioja.es/descarga/articulo/1985307.pdf>

Sorongun, F., Legowo, M., & Steph, S. (2021). *FinTech as The Emerging Technologies in Banking Industry: Past, Present, and Future*. *International Journal of Progressive Sciences and Technologies*, 371-378.

Staschen, S., & Meagher, P. (2022a). *3 Regulatory Challenges Posed by Platform-Based Finance*. Consultative Group to Assist the Poor [CGAP]: <https://www.cgap.org/blog/3-regulatory-challenges-posed-platform-based-finance>

Suárez, L. (2021). Instrumentos administrativos para el fomento de la innovación tecnológica en el sector financiero peruano. *Derecho PUCP*, (87), 183-229. <https://doi.org/10.18800/derechopucp.202102.006>

- Suárez, L. (2022). La problemática de emisión de tokens y plataformas de negociación de los mismos bajo la perspectiva del case law estadounidense. *Revista de derecho del mercado de valores*, (30), 112-132. <https://dialnet.unirioja.es/servlet/articulo?codigo=8501992>
- Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Luckow, A. (2021). Token economy. *Business & Information Systems Engineering*, 63, 457–478. <https://link.springer.com/article/10.1007/s12599-021-00684-1>
- Tantaleán, R. (2016). Tipología de las investigaciones jurídicas. *Derecho y Cambio Social*, 13(43), <https://dialnet.unirioja.es/servlet/articulo?codigo=5456267>.
- Tapia, A. (2018). *La Segunda Directiva de Servicios de Pago*. [bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/18/NOVIEMBRE/La\\_segunda\\_Directiva\\_de\\_Servicios\\_de\\_Pago.pdf](https://bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/18/NOVIEMBRE/La_segunda_Directiva_de_Servicios_de_Pago.pdf)
- Tapia, A. (2021a). Desafíos en la regulación y supervisión de los criptoactivos en la Unión Europea y en España. *Revista de Derecho del Mercado de Valores*, (28), <https://dialnet.unirioja.es/servlet/articulo?codigo=8053987>
- Vallet de Goytisolo, J. (1995). La analogía en el Derecho. *Estudios monográficos*. [https://www.boe.es/biblioteca\\_juridica/anuarios\\_derecho/abrir\\_pdf.php?id=ANU-C-1995-30103901088](https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-1995-30103901088)
- Velasco, L. (2021). El papel del derecho de la competencia en la era digital. *Revista de Estudios Europeos*, 78, 93-110. <https://dialnet.unirioja.es/servlet/articulo?codigo=7980449>
- Vidal-Tomás, D. (2022). The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Finance Research Letters*, (47), 102742. <https://doi.org/10.1016/j.frl.2022.102742>
- Wainer, A. (2015). Algunos determinantes de la restricción externa en la Argentina. *Universidad Nacional de General Sarmiento*.
- Wald, O., & Rochemont, S. (2019). *Understanding Central Bank Digital Currencies (CBDC)*. Institute and Faculty of Actuaries [IFoA].
- Wei, E., & Lin, W. (2021). IoT Piggy Bank for Money Saving Habit Instillation. *Journal of IT in Asia*, 09. <https://publisher.unimas.my/ojs/index.php/JITA/article/view/2860>
- Weinreb, L. L. (2005). *Legal reson: The use of analogy in legal argument*. Cambridge University Press.

Wharton School, Digital Asset Project, World Economic Forum. (2020). *DeFi Beyond de Hype. The Emerging World of Decentralized Finance*. <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>

Zetsche, D., Buckley, R., Arner, D., & Barberis, J. (2017). *From FinTech to TechFin: The Regulatory Challenges of Data-driven Finance*. European Banking Institute Working Paper Series: <http://hub.hku.hk/bitstream/10722/241271/1/Content.pdf>

Zetsche, D. A., Annunziata, F., Arner, D., & Buckley, R. (2020). *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*. European Banking Institute Working Paper Series.

Zetsche, D., & Woxholth, J. (2021). The DLT Sandbox under the Pilot-Regulation. *European Banking Institute*, 6-35. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3833766](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3833766)

Zetsche, D., Arner, D., & Buckley, R. (2020). Decentralized finance. *Journal of Financial Regulation*, 6(2),172-203. <https://doi.org/10.1093/jfr/fjaa010>

Zitelmann, E. (1922). Las lagunas del Derecho. *Revista general de legislación y jurisprudencia*, 70(140), 540-559.

Zunzunegui, F. (2020). *Aproximación al espacio controlado de pruebas (Regulatory Sandbox)*. *Regulación Financiera*. [http://www.rdmf.es/wp-content/uploads/2020/11/Zunzunegui-Aproximaci%C3%B3n-al-espacio-controlado-de-pruebas-Regulatory-Sandbox\\_WP-6-2020.pdf](http://www.rdmf.es/wp-content/uploads/2020/11/Zunzunegui-Aproximaci%C3%B3n-al-espacio-controlado-de-pruebas-Regulatory-Sandbox_WP-6-2020.pdf)

## Bibliografía – informes

- Accountancy Europe. (2020). *Response to the European commission's proposed regulation concerning digital operational resilience in the financial sector* (pp. 1-4). <https://www.accountancyeurope.eu/consultation-response/ecs-proposed-regulation-concerning-digital-operational-resilience-for-the-financial-sector/>
- Adrian, T. (2021). *BigTech in Financial Services*. International Monetary Fund [IMF]: <https://www.imf.org/en/News/Articles/2021/06/16/sp061721-BigTech-in-financial-services>
- Adrian, T., Lee, M., Mancini-Griffoli, T., & Martin, A. (2021). *Central Banks and Digital Currencies*. *Liberty Street Economics*. Federal Reserve Bank of New York.: <https://libertystreeteconomics.newyorkfed.org/2021/06/central-banks-and-digital-currencies/>
- Amstad, M. (2019). *Regulating FinTech: Objectives, Principles, and Practices*. Asian Development Bank Institute: <https://www.adb.org/publications/regulating-FinTech-objectives-principles-practices>
- Aramonte, S., Huang, W., & Schrimpf, A. (2021). *DeFi risks and the decentralisation illusion*. Bank of International Settlements. [https://www.bis.org/publ/qtrpdf/r\\_qt2112b.htm](https://www.bis.org/publ/qtrpdf/r_qt2112b.htm)
- Arner, D., Auer, R., & Frost, J. (2020). *Stablecoins: risks, potential and regulation*. Bank of International Settlements [BIS], Financial Stability Review: <https://www.bis.org/publ/work905.htm>
- Asociación Española de Compliance [ASCOM]. (2020). *Sector Financiero. RegTech*. ASCOM.
- Asociación Española de *FinTech* e *InsurTech* [AEFI]. (2019). *Libro blanco de InsurTech*. AEFI
- Asociación Española de *FinTech* e *InsurTech* [AEFI]. (2022). *Libro blanco de lending online*. AEFI.
- Asociación Española de *FinTech* e *InsurTech*. (2020). *Libro blanco de PayTech. La evolución del sector PayTech y nuevos retos regulatorios*. [https://www.asociacionFinTech.es/wp-content/uploads/2020/12/AEFI\\_Libro-Blanco-PayTech-2020\\_Diciembre-2020-1.pdf](https://www.asociacionFinTech.es/wp-content/uploads/2020/12/AEFI_Libro-Blanco-PayTech-2020_Diciembre-2020-1.pdf)

Auer, R. (2019). *Embedded supervision: how to build regulation into blockchain finance*. Working Papers No. 811, Bank of International Settlements [BIS], Monetary and Economic Department (pp. 1-31): <https://www.bis.org/publ/work811.pdf>

Bache, I. W. (2021). *FinTech, BigTech and cryptos- will new technology render banks obsolete?* Central Bank of Norway (pp. 1-7): <https://www.bis.org/review/r210511b.htm>

Bank of International Settlements [BIS]. (2018). *Annual Economic Reports 2018*. <https://www.bis.org/publ/arpdf/ar2018e5.pdf>

Bank of International Settlements [BIS]. (2019a). *III. Big tech in finance: opportunities and risks*. Annual Economic Report 2019 (pp.1-26): <https://www.bis.org/publ/arpdf/ar2019e3.htm>

Bank of International Settlements [BIS]. (2019b). *PS4: Participation in selected payment systems*. <https://stats.bis.org/statx/srs/table/PS4>

Bank of International Settlements [BIS]. (2020a). *Enhancing cross border payments: building blocks of a global roadmap*. <https://www.bis.org/cpmi/publ/d193.htm>

Bank of International Settlements [BIS]. (2020b). *Basel Framework. LCR. LCR 30*. [https://www.bis.org/basel\\_framework/chapter/LCR/30.htm?tldate=20281012&inforce=20191215&published=20200605](https://www.bis.org/basel_framework/chapter/LCR/30.htm?tldate=20281012&inforce=20191215&published=20200605)

Bank of International Settlements [BIS]. (2020c). *Central banks and payments in the digital era*. BIS Annual Economic Report 2020: <https://www.bis.org/publ/arpdf/ar2020e3.pdf>

Bank of International Settlements [BIS]. (2021a). *Pushing the frontiers of payments: towards faster, cheaper, more transparent and more inclusive cross border payments*. Committee on Payments and Markets Infrastructures: <https://biscpmi.navus.io/950/page/event-description>

Basel Committee on Banking Supervision & Bank of International Settlements. (2018). *Implications of FinTech developments for banks and bank supervisors*. <https://www.bis.org/bcbs/publ/d431.htm>

Basel Committee on Banking Supervision. (2022). *Prudential treatment of Cryptoassets Exposures*. <https://www.bis.org/bcbs/publ/d545.htm>

BBVA. (2022). *¿Qué es el banking as a service?* <https://www.bbva.com/es/que-es-banking-as-a-service/>

Berger, S. (2022, March 14). *MiCA final compromises on behalf of MEP Berger*. Bitcoin. <https://bitcoin.fr/wp-content/uploads/2022/03/MiCA-Compromises-v9-9-March-2022.pdf>

Bullman, D., Klemm, J., & Pinna, A. (2019). *In seach for stability in crypto-assets: are stablecoins the solution?* Occasional Paper Series, European Central Bank [ECB]: <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf?321f6bf14960e6f604725be5a466957b>

Bundesamt für Sicherheit in der Informationstechnik. (2021). *A Brief guideline on Self-Sovereign Identities (SSI) with special regard to the distributed ledger technology (DLT)*. [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/guideline\\_self-sovereign\\_identities.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/guideline_self-sovereign_identities.pdf?__blob=publicationFile&v=2)

Busch, K. (2022). *Non-Fungible Tokens (NFTs)*. Congressional Research Service.

Capgemini. (2021). *Retail banking top trends 2021. Drivers, oportunities and risks shaping financial services*. [https://www.capgemini.com/wp-content/uploads/2020/11/Retail-Banking-Trends\\_2021\\_Web.pdf](https://www.capgemini.com/wp-content/uploads/2020/11/Retail-Banking-Trends_2021_Web.pdf)

Carney, M. (2019). *Enable, Empower, Ensure: A New Finance for the New Economy*. Bank of England: <https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/enable-empower-ensure-a-new-finance-for-the-new-economy-speech-by-mark-carney>

Coalition of Automated Legal Applications. (2021). *Model law for automated decentralized autonomous organizations (DAOs)*. <https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf>

Comisión Europea. (2013). *Report from the Commission to the European Parliament and the Council on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation (EC) No 924/2009 on cross-border payments in the Community*. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52013DC0549>

Comisión Europea. (2020a). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on a Digital Finance Strategy for the EU*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>



Comisión Europea. (2020c). *Servicios financieros: marco regulador de la UE para los criptoactivos. Comentarios. Comentario F1292738*: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Servicios-financieros-marco-regulador-de-la-UE-para-los-criptoactivos/F1292738\\_es](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Servicios-financieros-marco-regulador-de-la-UE-para-los-criptoactivos/F1292738_es)

Comisión Nacional del Mercado de Valores [CNMV]. (2020). *Atención de reclamaciones y consultas de los inversores. Memoria 2020*. CNMV

Comisión Nacional del Mercado de Valores [CNMV]. (2020). *El mercado de valores y los productos de inversión. Manual para universitarios*. CNMV

Comisión Nacional del Mercado de Valores [CNMV]. (2021). *Informe anual sobre los mercados de valores y su actuación 2020*. [https://www.cnmv.es/DocPortal/Publicaciones/Informes/Informe\\_Anual\\_2020.pdf](https://www.cnmv.es/DocPortal/Publicaciones/Informes/Informe_Anual_2020.pdf)

Comisión Nacional del Mercado de Valores [CNMV]. (2021). *Líneas estratégicas de la CNMV 2021-2022. Plan de actividades 2021*. Comisión Nacional del Mercado de Valores.

Comisión Nacional del Mercado de Valores [CNMV]. (2022). *Estudio sobre las criptomonedas y la efectividad de las medidas impulsadas por CNMV*. CNMV.

Comité Económico y Social Europeo. (2021). *Dictamen del Comité Económico y Social Europeo sobre: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (EU) 2019/1937 (COM (2020) 593 final-2020/0265(COD))*.

Commission de Surveillance du Secteur Financier [CSSF]. (2022). *Distributed Ledger Technologies & Blockchain. Technological Risks and Recommendations for the Financial Sector*. [https://www.cssf.lu/wp-content/uploads/DLT\\_WP.pdf](https://www.cssf.lu/wp-content/uploads/DLT_WP.pdf)

Commission of European Communities. (1999). *Implementing the framework for financial markets: action plan. COM (1999) 232*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51999DC0232&from=RO>

Committee on Payments and Markets Infrastructures [CPMI]. (2018). *Central bank digital currencies*. <https://www.bis.org/cpmi/publ/d174.pdf>

Committee on Payments and Markets Infrastructures [CPMI]. (2020). *Enhancing cross-border payments: building blocks of a global roadmap. Stage 2 report to the G20 – technical background report*. <https://www.bis.org/cpmi/publ/d193.pdf>

Crisanto, J., Ehrentraud, J., Fabian, M., & Monteil, A. (2022). *Big tech interdependencies – a key policy blind spot*. Bank of International Settlements.

Doerr, S., Gambacorta, L., & Serena, J. M. (2021). *Big data and machine learning in central banking*. BIS Working Papers No. 930. Bank of International Settlements (BIS), Monetary and Economic Department.

Enria, A. (2018). *Designing a Regulatory and Supervisory Roadmap for FinTech*. European Banking Authority [EBA]: <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2151635/9aaf2e3f-e443-4d19-a1f5-fa57847e3e6a/Andrea%20Enria%27s%20speech%20on%20FinTech%20at%20Copenhagen%20Business%20School%20090318.pdf?retry=1>

Eskandari, S., Salehi, M., Gu, W., & Clark, J. (2021). *SoK: Oracles from the Ground Truth to Market Manipulation*. <https://arxiv.org/abs/2106.00667>

Euro Banking Association. (2017a). *Open Banking: advancing customer-centricity. Analysis and overview*. [https://www.abe-eba.eu/media/azure/production/1355/eba\\_open\\_banking\\_advancing\\_customer-centricity\\_march\\_2017.pdf](https://www.abe-eba.eu/media/azure/production/1355/eba_open_banking_advancing_customer-centricity_march_2017.pdf)

European Banking Authority [EBA]. (2019b). *EBA Report on the impact of FinTech on payment institutions' and e-money institutions' business models*. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/32ff1cbb-a6c3-4a01-94f2-4d129386fa0a/EBA%20thematic%20report%20on%20the%20impact%20of%20FinTech%20on%20PIs%27%20and%20EMIs%27%20business%20models.pdf?retry=1>

European Banking Authority [EBA]. (2019c). *Report with advice for the European Commission on Crypto-assets*. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf>

European Banking Authority [EBA]. (2021a). *Analysis of RegTech in the EU Financial Sector*. [https://www.eba.europa.eu/sites/default/documents/files/document\\_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf](https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf)

European Banking Authority [EBA]. (2021c). *Report on the use of digital platforms in the EU banking and payments sector*. EBA/REP/2021/26. EBA.

European Banking Authority [EBA]. (2021d). *Revised Guidelines on major incident reporting under PSD2*. EBA.

European Central Bank [ECB]. (2020b). *Report on a digital euro*. [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf#page=4](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf#page=4)

European Central Bank [ECB]. (2021b). *Report on the public consultation on a digital euro*. [https://www.ecb.europa.eu/paym/digital\\_euro/html/pubcon.en.html](https://www.ecb.europa.eu/paym/digital_euro/html/pubcon.en.html)

European Central Bank [ECB]. (2022a). *Decrypting financial stability risks in crypto-asset markets*. Financial Stability Review: [https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205\\_02~1cc6b111b4.en.html](https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html)

European Central Bank and Bank of Japan. (2019). *STELLA – joint research project of the European Central Bank and the Bank of Japan*. <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf>

European Commission [EC]. (2020f). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social committee and the committee of the regions on a Retail Payments Strategy for the EU*.

European Commission [EC]. (2018). *Communication from the commission to the european parliament, the council, the european central bank, the european economic and social committee and the committee of the regions FinTech Action plan: For a more competitive and innovative European financial*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109>

European Commission [EC]. (2020c). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, A European strategy for data, COM (2020) 66 final*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>

European Commission [EC]. (2021a). *Commission staff working document impact assessment report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Id. SWD/2021/124 final*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>

European Commission [EC]. (2021b). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions 2030 Digital Compass: the European way for the Digital*

*Decade.* COM/2021/118 *final.* <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118>

European Commission [EC]. (2021d). *Commission staff working document. Impact assessment report accompanying the proposal for a Directive of the European Parliament and the Council on consumer credits.* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2021:170:FIN&locale=en>

European Insurance and Occupational Pensions Authority [EIOPA] . (2019). *Report on best practices on licensing requirements, peer-to-peer insurance and the principle of proportionality on an InsurTech context.* Publications Office of the European Union.

European Insurance and Occupational Pensions Authority [EIOPA]. (2020). *Annual Report 2020.* EIOPA.

European Insurance and Occupational Pensions Authority [EIOPA]. (2021). *Open insurance: accessing and sharing insurance-related data.* [https://www.eiopa.europa.eu/content/open-insurance-accessing-and-sharing-insurance-related-data\\_en](https://www.eiopa.europa.eu/content/open-insurance-accessing-and-sharing-insurance-related-data_en)

European Parliament [EP]. (2021). *Establishing a framework for a European Digital Identity.*

European Parliament [EP]. (2021). *Understanding initial coin offerings.* [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS\\_BRI\(2021\)696167\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696167/EPRS_BRI(2021)696167_EN.pdf)

European Securities and Markets Authority [ESMA]. (2019). *Advice. Initial Coin Offerings and Crypto-Assets.* [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf)

European Securities and Markets Authority [ESMA]. (2021). *MiFID II review report on the functioning of Organised Trading Facilities (OTF).* [https://www.esma.europa.eu/sites/default/files/esma70-156-4225\\_mifid\\_ii\\_final\\_report\\_on\\_functioning\\_of\\_otf.pdf](https://www.esma.europa.eu/sites/default/files/esma70-156-4225_mifid_ii_final_report_on_functioning_of_otf.pdf)

European Supervisory Authorities. (2019). *Joint Advice of the European Supervisory Authorities To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector.*

European Union. (2016). *Towards European Supervisory Convergence. the Joint Committee of the European Supervisory Authorities.* European Union.

Expert Group on Regulatory Obstacles to Financial Innovation [ROFIEG]. (2019). *30 recommendations on regulation, innovation and finance*. [https://ec.europa.eu/info/sites/default/files/business\\_economy\\_euro/banking\\_and\\_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation\\_en.pdf](https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf)

Financial Action Task Force [FATF]. (2012/2020). *International standards on combating money laundering and the financing terrorism and proliferation. The FATF recommendations*. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

Financial Action Task Force [FATF]. (2020a). *12 Month Review of Revised FATF Standards - Virtual Assets and VASPs*. FATF.

Financial Action Task Force [FATF]. (2020b). *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf>

Financial Action Task Force [FATF]. (2021a). *International standards on combating money laundering and the financing terrorism proliferation. The FATF recommendations*. FATF.

Financial Action Task Force [FATF]. (2021b). *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>

Financial Action Task Force [FATF]. (2021c). *Virtual assets and virtual asset service providers*. FATF.

Financial Action Task Force [FATF]. (2023) *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*

Financial Conduct Authority [FCA]. (2016). *Copy trading*. <https://www.fca.org.uk/firms/copy-trading>

Financial Stability Board [FSB]. (2013). *Principles for An Effective Risk Appetite Framework*. [https://www.fsb.org/wp-content/uploads/r\\_131118.pdf](https://www.fsb.org/wp-content/uploads/r_131118.pdf)

Financial Stability Board [FSB]. (2019). *FinTech and market structure in financial services: Market developments and potential financial stability implications*. FSB.

Financial Stability Board [FSB]. (2020a). *Effective Practices for Cyber Incident Response and Recovery*. <https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/>

Financial Stability Board [FSB]. (2020b). *Enhancing Cross-border Payment. Stage 3 roadmap*.

Financial Stability Board [FSB]. (2020c). *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*. Final Report and High-Level Recommendations, Financial Stability Board (FSB). <https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/>

Financial Stability Board [FSB]. (2020d). *Enhancing Cross-border Payments. Stage 1 report to the G20*. <https://www.fsb.org/wp-content/uploads/P090420-1.pdf>

Financial Stability Board [FSB]. (2020e). *Addressing the regulatory, supervisory and oversight challenges raised by global stablecoin arrangements*. <https://www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document/>

Financial Stability Board [FSB]. (2021). *FinTech*. <https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/FinTech/>

G7 Working Group on Stablecoins. (2019). *Investigating the impact of global stablecoins*. <https://www.bis.org/cpmi/publ/d187.pdf>

Global Digital Finance. (2022). *Cryptoasset safekeeping and custody*.

Guillaume, F., & Riva, S. (2022). *Model Law for DAOs – a legal regime adapted to a new type of digital company*. LexTech Institute. University of Neuchâtel: <https://www.lextechinstitute.ch/loi-type-sur-les-daos-un-regime-juridique-adapte-aux-nouvelles-formes-de-societes-numeriques/?lang=en>

Joint Committee of European Supervisory Authorities [JCESAs]. (2021). *2022 Work Programme*. [https://www.eba.europa.eu/sites/default/documents/files/document\\_library/About%20Us/Governance%20structure/JC/work%20programme/1020914/JC%202021%2034%20%28Joint%20Committee%20Work%20Programme%202022%20-%20final%29.pdf](https://www.eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Governance%20structure/JC/work%20programme/1020914/JC%202021%2034%20%28Joint%20Committee%20Work%20Programme%202022%20-%20final%29.pdf)

Maupin, J. (2017). *Blockchains and the G20: Building and Inclusive, Transparent and Accountable Digital Economy*. Center for International Governance Innovation Policy Brief: <https://www.cigionline.org/static/documents/documents/PB%20no.101.pdf>

Mazzucato, M., & Wray, L. (2015). *Financing the Capital Development of the Economy: A Keynes-Schumpeter-Minsky Synthesis*. Levy Economics Institute: [https://www.levyinstitute.org/pubs/wp\\_837.pdf](https://www.levyinstitute.org/pubs/wp_837.pdf)

MENA FinTech Association. (2021). *Open Finance. A framework for the Arab region is more than a question of scope*. <https://www.amf.org.ae/sites/default/files/publications/2022-01/open-finance-framework-arab-region-more-question-scope.pdf>

OECD. (2018). *G20/OECD INFE Policy Guidance on Digitalisation and Financial Literac*. <https://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf>

OECD iLibrary. (2020). *Regulatory Policy in the Slovak Republic: Towards Future-Proof Regulation*. Innovative approaches to support future-proofing regulation: <https://www.oecd-ilibrary.org/sites/94d061e5-en/index.html?itemId=/content/component/94d061e5-en>

OICV-IOSCO. (2020). *Global Stablecoin Initiatives*. <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>

PricewaterhouseCoopers International Limited. (2021). *DeFi: defining the future of finance*. <https://www.pwc.ch/en/insights/digital/defi-defining-the-future-of-finance.html>

Restoy, F. (2021). *FinTech regulation: how to achieve a level playing field*. Occasional Paper, Financial Stability Institute [FSI]: <https://www.bis.org/fsi/fsipapers17.pdf>

Singapore FinTech Association y BCG. (2020). *Digital challenger banks*. <https://camaraFinTech.com.ar/wp-content/uploads/2020/11/Digital-Challenger-Banks.pdf>

Su, E. (2020). *Digital Assets and SEC Regulation*. US Congressional Research Service.

Sveriges Riksbank. (2021). *E-krona pilot. Phase 1*. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf>

The City of London. (2021). *Kalifa Review of UK FinTech. Executive Summary*. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/971371/KalifaFinTechReview\\_ExecSumm.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971371/KalifaFinTechReview_ExecSumm.pdf)

The Committee of Wise Men. (2001). *Final report of the Committee of Wise Men on the regulation of european securities markets*. [https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy\\_report.pdf](https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy_report.pdf)

The World Bank Group. (2020). *How Regulators Respond to FinTech*. International Bank for Reconstruction and Development.

U.S. Department of State. (2021). *Threat finance countermeasures. De-risking*. <https://www.state.gov/de-risking/>

Withian, W. (2020). *Q-3 2020 Layer 1 review report*. Messari.

World Economic Forum [WEF]. (2021). *Decentralized Finance (DeFi) Policy-Maker Toolkit*. <https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit/>

Zamil, R., & Lawson, A. (2022). *Gatekeeping the gatekeepers: when big techs and the FinTechs own banks – benefits, risks and policy options*. Financial Stability Institute of the Bank of International Settlements. <https://www.bis.org/fsi/publ/insights39.htm>



## Bibliografía – otros

- Aave. (2022). *Flash loans (p. 1)* <https://docs.aave.com/faq/flash-loans>
- Accenture Research. (2020). *Tendencias y oportunidades en la industria de medios de pago en Argentina* (p. 11). [https://www.accenture.com/\\_acnmedia/PDF-138/Accenture-Transformacion-Medios-de-Pago-Version-Corta.pdf](https://www.accenture.com/_acnmedia/PDF-138/Accenture-Transformacion-Medios-de-Pago-Version-Corta.pdf)
- Accenture. (2014). *White Labeling: “White Hot” Opportunity for Payments Players* (pp. 1-2).  
<https://www.accenture.com/content/dam/accenture/final/industry/banking/document/Accenture-Payments-Gets-Personal.pdf>
- Allen, C. (2016). *The path to self-sovereign identity*. Life with Alacrity (pp. 1-15).  
<http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- Anchorage Digital. (2022). *Digital Asset Custody. A primer for institutions* (pp. 1-60).  
<https://www.anchorage.com/marketing/Building-Crypto-Products-Primer.pdf>
- Arias, M. (2015). *Sobre copy trade y social trading. Postura de la CNMV - social trading*.  
<https://www.rankia.com/foros/bolsa/temas/3022195-copy-trade-social-trading-postura-cnmv>
- Association for Financial Markets in Europe [AFME]. (2022). *Comments to the ESMA Pilot*. AFME.
- Bailey, A. (2021). Innovation to serve the public interest. *Speech at the City UK Annual Conference*. <https://www.bis.org/review/r210615d.htm>
- Banco de España. (2008). *TARGET2-Banco de España*.  
[https://www.bde.es/bde/es/areas/sispago/sis\\_pago\\_may/TARGET2-Banco\\_de/](https://www.bde.es/bde/es/areas/sispago/sis_pago_may/TARGET2-Banco_de/)
- Banco de España. (2020). *Servicio de información sobre cuentas y de iniciación de pagos, no confundas* (pp.1-2).  
[https://clientebancario.bde.es/pcb/es/blog/informacion\\_cuentas\\_iniciacion\\_pagos.html](https://clientebancario.bde.es/pcb/es/blog/informacion_cuentas_iniciacion_pagos.html)
- Banco de España. (2021). *Los sistemas de liquidación en España* (pp.12).  
[https://www.bde.es/bde/es/areas/sispago/Una\\_vision\\_gener/Los\\_sistemas\\_de\\_/Los\\_sistemas\\_de\\_c17a344baded821.html](https://www.bde.es/bde/es/areas/sispago/Una_vision_gener/Los_sistemas_de_/Los_sistemas_de_c17a344baded821.html)
- Banco de España. (2022). *Supervisar la solvencia de entidades* (pp.1-2).  
[https://www.bde.es/bde/es/secciones/sobreelbanco/funcion/Supervisar\\_la\\_s\\_40792d8e17a821.html](https://www.bde.es/bde/es/secciones/sobreelbanco/funcion/Supervisar_la_s_40792d8e17a821.html)

Bank of International Settlements [BIS]. (2021b). *BIS Innovation Summit 2021: How can central banks innovate in the digital age?* [https://www.bis.org/events/bis\\_innovation\\_summit\\_2021/agenda.htm](https://www.bis.org/events/bis_innovation_summit_2021/agenda.htm)

Bank of International Settlements [BIS]. (2021c). *Glossary*. [https://www.bis.org/cpmi/publ/d00b.htm?&selection=149&scope=CPMI&c=a&base=term#:~:text=zero%20hour%20rule-,straight%20through%20processing%20\(STP\),re%20keying%20or%20reformatting%20data.](https://www.bis.org/cpmi/publ/d00b.htm?&selection=149&scope=CPMI&c=a&base=term#:~:text=zero%20hour%20rule-,straight%20through%20processing%20(STP),re%20keying%20or%20reformatting%20data.)

BankID. (2021). *This is BankID*. <https://www.bankid.com/en/om-bankid/detta-ar-bankid>

Banxico. (2021). *Introducción a los sistemas de pago*. <https://www.banxico.org.mx/sistemas-de-pago/introduccion-sistemas-pago-tr.html>

Barclays. (2017). *From the archives: the ATM is 50*. <https://home.barclays/news/2017/06/from-the-archives-the-atm-is-50/#:~:text=That%20restriction%20was%20lifted%20fifty,Bank%20in%20Enfield%20C%20north%20London.>

Bartz, T. (2021). *Interview with Fabio Panetta, Member of the Executive Board of the ECB, conducted by Tim Bartz*. Interview with Der Spiegel: <https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210209~af9c628e30.en.html>

BBC News Mundo. (2021). *La curiosa historia de cómo nació el cajero automático*. <https://www.bbc.com/mundo/noticias-40417156>

Belvo. (2021). *Economía colaborativa*. <https://belvo.com/es/productos/economia-colaborativa/>

Betaalvereniging Nederland. (2021). *Feedback on the draft Digital Operational Resilience Act*. [https://www.betaalvereniging.nl/wp-content/uploads/Feedback-on-draft-proposal-DORA\\_final.pdf](https://www.betaalvereniging.nl/wp-content/uploads/Feedback-on-draft-proposal-DORA_final.pdf)

Bison Trails. (2021). *Infrastructure and Design of Central Bank Digital Currencies*. <https://www.forbes.com/sites/vipinbharathan/2021/05/19/bison-trails-publishes-a-research-report-on-central-bank-digital-currencies/?sh=50e2995a655b>

Bit2me academy. (2022). *¿Qué son DApps?* <https://academy.bit2me.com/que-son-las-dapps/>

Bit2me academy. (2023). *¿Qué es un token ERC-1155 en Ethereum?*  
<https://academy.bit2me.com/que-es-token-erc-1155/>

Bit2me. (2021). *¿Qué es DPoS?* <https://academy.bit2me.com/que-es-dpos/>

Bit2me. (2022a). *¿Qué es staking?* Bit2me Academy: <https://academy.bit2me.com/que-es-staking/>

Bit2me. (2022b). *¿Qué es un airdrop?* Bit2me Academy: <https://academy.bit2me.com/que-es-un-airdrop-criptomonedas/>

Bitpanda Financial Services. (2022). *Cost transparency document.*  
[https://cdn.bitpanda.com/media/documents/securities/en-cost-transparency-document.pdf?\\_ga=2.111248000.564110927.1648292482-843279742.1648292482&\\_gac=1.121098618.1648292482.Cj0KCQjw8\\_qRBhCXARISAE2AtRauKMeHdDjc2obqc\\_1t\\_--\\_58JQVHcYCX-WQZ0T1t7KVexQIWtONegaApA](https://cdn.bitpanda.com/media/documents/securities/en-cost-transparency-document.pdf?_ga=2.111248000.564110927.1648292482-843279742.1648292482&_gac=1.121098618.1648292482.Cj0KCQjw8_qRBhCXARISAE2AtRauKMeHdDjc2obqc_1t_--_58JQVHcYCX-WQZ0T1t7KVexQIWtONegaApA).

Biurrun, A. (2022). *Estafas a través de plataformas de inversión falsas: qué son, cómo detectarlas y actuar.* La razón: <https://www.larazon.es/tecnologia/20220316/r37agk4iwzbjpop6zv2bd2fmei.html>

Boar, C., & Wehrli, A. (2021). *Ready, steady, go? – Results of the third BIS survey on central bank digital currency.* *BIS Papers No 114.*  
<https://www.bis.org/publ/bppdf/bispap114.pdf>

Bofinger, P. (2021). *The Future of Central Bank Digital Currencies (CBDC): Should the ECB issue a Digital Euro?* <https://www.youtube.com/watch?v=KtDxOGyFA7Y>

Borio, C., Claessens, S., & Tarash, N. (2022). *Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs.*  
<https://www.bis.org/fsi/fsipapers19.htm>

*Britannica.* (2 de febrero de 2022). *Bloomberg News.*  
<https://www.britannica.com/topic/Bloomberg-News>

Buterin, V. (2014). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide.* Ethereum foundation blog: <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>

Carstens, A. (2018). *Big tech in finance and new challenges for public policy.* FT Banking Summit: <https://www.bis.org/speeches/sp181205.htm>

Caudevilla, O. (2021a). *Hong Kong should play a key role in digital yuan rollout*. China Daily: <https://www.chinadailyhk.com/article/160251#Hong-Kong-should-play-a-key-role-in-digital-yuan-rollout>

Caudevilla, O. (2021b). *Las CBDCs en el mundo: el Yuan Digital. ¿Hacia un euro digital también?* Webinar Instituto Estudios Bursátiles [IEB].

CBINSIGHTS. (2021). *What are Stablecoins?* <https://www.cbinsights.com/research/report/what-are-stablecoins/#:~:text=A%20stablecoin%20is%20typically%20a,value%20of%20an%20underlying%20asset>.

Ceyskens, J. (2021). *Electronic Money Association Response to the EC consultation on Proposal for a regulation on digital operational resilience for the financial sector-COM (2020) 595*.

Chainalysis. (2022). *The Chainalysis state of Web 3.0 report*. <https://go.chainalysis.com/2022-web3-report.html>

Chainalysis. (2021). *The 2021 Global Crypto Adoption Index*. <https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index>

Charnley, B. (2021). *From Open Banking to Open Data: Australia's Open Finance Journey Begins!* <https://medium.com/open-finance-australia/from-open-banking-to-open-data-australias-open-finance-journey-begins-ce730f3270a7>

Cherrayil, N. K. (2021). *59% of millennials happy to opt for digital-only banks*. <https://www.techchannel.news/17/06/2021/59-of-millennials-happy-to-opt-for-digital-only-banks/>

Circle. (2022). *Euro Coin. A euro stablecoin backed by full reserves*: <https://www.circle.com/en/euro-coin>

Clark, T. (2021). *What is FinTech? FinTech Foundations and Overview*. The Hong Kong University of Science and Technology: <https://www.coursera.org/learn/FinTech>

Clifford Chance. (2021). *Non-fungible tokens: the global legal impact*. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf>

Cœuré, B. (2018). *The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs*. Economics of Payments IX conference: [https://www.ecb.europa.eu/pub/pdf/annex/ecb.sp181115\\_slides.en.pdf](https://www.ecb.europa.eu/pub/pdf/annex/ecb.sp181115_slides.en.pdf)

Cognizant. (2016). *How Banking as a Service will keep banks digitally relevant and growing*. <https://www.slideshare.net/cognizant/how-banking-as-a-service-will-keep-banks-digitally-relevant-and-growing>

Coin ATM Radar. (2022). *Bitcoin ATM Installations Growth*. <https://coinatmradar.com/charts/growth/>

Coinmarketcap. (2022). *DYCO (Dinamic Coin Offering)*. <https://coinmarketcap.com/alexandria/glossary/dyco-dynamic-coin-offering>

Coinmarketcap. (s.f.). *Initial Dex Offering (IDO)*. <https://coinmarketcap.com/alexandria/glossary/initial-dex-offering>

Comisión Europea. (2021c). *La Comisión revisa las normas de la UE sobre el crédito al consumo y la seguridad de los productos*. [https://ec.europa.eu/commission/presscorner/detail/es/ip\\_21\\_3242](https://ec.europa.eu/commission/presscorner/detail/es/ip_21_3242)

Comisión Europea. (2021d). *Request to EBA, eiopa and esma for technical advice on digital finance and related issues*. [https://ec.europa.eu/info/sites/default/files/business\\_economy\\_euro/banking\\_and\\_finance/documents/210202-call-advice-esas-digital-finance\\_en.pdf](https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/210202-call-advice-esas-digital-finance_en.pdf)

Comisión Europea. (2022). *Una Europa Adaptada a la Era Digital: nuevas normas para las plataformas online*. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms\\_es](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_es)

Comisión Nacional Bancaria y de Valores de México [CNBV]. (2020). *Aviso sobre entidades autorizadas y en proceso de autorización*. [https://www.gob.mx/cms/uploads/attachment/file/597033/CNBV\\_Aviso\\_sobre\\_entidades\\_autorizadas.pdf](https://www.gob.mx/cms/uploads/attachment/file/597033/CNBV_Aviso_sobre_entidades_autorizadas.pdf)

Compound. (2019). *Compound: The Money Market Protocol*. <https://compound.finance/documents/Compound.Whitepaper.pdf>

Conesa, C. (2021). *CNMV: FinTech & Ciberseguridad. Encuentro con el sector*. <https://www.cnmv.es/Portal/FinTech/Jornadas.aspx>

Consejo Europeo. (2022a). *Infografía - EU system of financial supervision*. <https://www.consilium.europa.eu/es/infographics/financial-supervision-architecture/>

Consejo Europeo. (2022b). *Unión Bancaria*. <https://www.consilium.europa.eu/es/policies/banking-union/>

Council of the European Union. (2022). *Digital finance: agreement reached on European crypto-assets regulation (MiCA)*.  
<https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>

Crunchbase. (2021c). *Crunchbase*.  
[https://www.crunchbase.com/organization/rappi/company\\_financials](https://www.crunchbase.com/organization/rappi/company_financials)

Crunchbase. (2022). *Organization: WeChat*.  
<https://www.crunchbase.com/organization/we-chat>

CryptoCurrency Facts. (2021). *Understanding Hard Forks in Cryptocurrency*.  
<https://cryptocurrencyfacts.com/understanding-hard-forks-cryptocurrency/>

Cuatrecasas. (2011). *Negocios en China: aspectos legales y fiscales*.  
[https://www.cuatrecasas.com/media\\_repository/docs/esp/negocios\\_en\\_china\\_aspectos\\_legales\\_y\\_fiscales\\_869.pdf](https://www.cuatrecasas.com/media_repository/docs/esp/negocios_en_china_aspectos_legales_y_fiscales_869.pdf)

Daian, P., Kell, T., Miers, I., & Juels, A. (2 de July de 2018). *On-Chain Vote Buying and the Rise of Dark DAOs*. Hacking, Distributed:  
<https://hackingdistributed.com/2018/07/02/on-chain-vote-buying/>

De Francisco, S., Casais, M., & Desmet, P. (2014). *Feeding your piggy bank with intentions: a study on saving behaviour, saving strategies and happiness*. Proceedings of the Colors of Care: The 9th International Conference on Design & Emotion:  
<https://diopd.org/wp-content/uploads/2015/11/DeFrancisco-FeedingYourPiggyBank2014.pdf>

Deloitte Consulting A.G. (2015). *Swiss Banking Models of the Future. Embarking to New Horizons*.  
<https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/financial-services/ch-en-fs-bank-of-tomorrow.pdf>

Deloitte tax and consulting Sarl. (2020). *Are central bank digital currencies (CBDC) the money of tomorrow?*  
<https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/lu-are-central-bank-digital-currencies.pdf>

Deloitte y Dubai Financial Services Authority. (2022). *A Market Overview of Custody for Digital Assets. Digital Custodian Whitepaper*. Deloitte.

Deloitte. (s.f.). *How blockchain can reshape trade finance*. <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/trade-finance-placemat.pdf>

Dentons. (2020). *Meet MiCA - The EU pushes forward its proposal for its Markets in Crypto-Assets Regulation plus a pilot regime for DLT infrastructure*. <https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/november/13/background-briefing-meet-mica>

Deutsche Börse Group. (2021). *Position paper on the European Commission's legislative proposals on Dora*. <https://www.deutsche-boerse.com/resource/blob/2642592/ba122a65102780a12b44a6798518657f/data/Feb2021-DORA-response.pdf>

Deutsche Bundesbank. (2021). *Amplus*. <https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/veroeffentlichungen/amplus/amplus-859572>

Digital Asset Association Austria. (2021). *Feedback on the Proposal for regulation on markets in crypto-assets and on the Proposal for a pilot regime for market infrastructures based on distributed ledger technology*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594>

Écija. (2022). *Metaverso: una primera aproximación jurídica y cuestiones por resolver*. Écija.

Eichler, S., & Thum, M. (2019). *Libra – Totengräberin für gescheiterte Währungen, Herausforderung für gute Regulierung*. *Alemania: ifo Schnelldienst 17 / 2019*. <https://www.ifo.de/DocDL/sd-2019-17-eichler-thum-kryptowaehrungen-bitcoin-libra-2019-09-12.pdf>

Ethereum. (2021a). *Ethereum Whitepaper*. <https://ethereum.org/en/whitepaper/>

Ethereum. (2021b). *Proof-of-Stake (POS)*. <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>

European Banking Authority [EBA]. (2017b). *Discussion paper on the EBA's approach to financial technology (FinTech)*. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20FinTech%20%28EBA-DP-2017-02%29.pdf?retry=1>

European Banking Authority [EBA]. (2021b). *EBA publishes final revised Guidelines on major incident reporting under PSD2*. <https://www.eba.europa.eu/eba-publishes-final-revised-guidelines-major-incident-reporting-under-psd2>

European Banking Authority [EBA]. (2022a). *2019\_4594 Definition of an electronic remote payment transaction*. [https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019\\_4594](https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4594)

European Banking Authority [EBA]. (2022b). *Joint Committee*. <https://www.eba.europa.eu/about-us/organisation/joint-committee>

European Banking Authority [EBA]. (2022c). *Payment Institutions Register*. <https://euclid.eba.europa.eu/register/pir/search>

European Banking Federation [EBF]. (2021a). *EBF Position Paper on the European Commission's proposal for a Regulation on digital operational resilience for the financial sector (DORA)*. Brussels. <https://www.ebf.eu/innovation-cybersecurity/european-commissions-proposal-for-a-regulation-on-digital-operational-resilience-for-the-financial-sector-ebf-position/>

European Banking Federation [EBF]. (2022b). *DP on FinTech. Submission number 5*. <https://www.eba.europa.eu/node/82086/submission/63904#:~:text=The%20principle%20of%20%E2%80%9Csame%20services,technological%20developments%20and%20business%20models>

European Banking Federation [EBF]. (2022c). *EBF response to European Commission Consultation on the review of the revised payment services Directive (PSD 2)*. <https://www.ebf.eu/wp-content/uploads/2022/07/EBF-Response-to-Commission-Consultation-on-PSD2.pdf>

European Central Bank [ECB]. (2020a). *ECB welcomes initiative to launch new European payment solution*. Press release: <https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200702~214c52c76b.es.html>

European Central Bank [ECB]. (2020c). *Sweden joins ECB's instant payments settlement platform*. [https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200403\\_1~302d8928e3.en.html](https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200403_1~302d8928e3.en.html)

European Central Bank [ECB]. (2021a). *Glossary*. <https://www.ecb.europa.eu/services/glossary/html/glossb.en.html>



European Central Bank [ECB]. (2022b). *Hitos*.  
<https://www.bankingsupervision.europa.eu/about/milestones/html/index.es.html>

European Central Bank [ECB]. (2022c). *How does banking supervision work?*  
<https://www.bankingsupervision.europa.eu/banking/approach/cycle/html/index.es.html>

European Central Bank [ECB]. (2022d). *Single Supervision Mechanism*.  
<https://www.bankingsupervision.europa.eu/about/thessm/html/index.en.html>

European Commission [EC]. (2022). *Targeted consultation on the review of the revised payment services Directive (PSD 2)*. [https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review\\_en](https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en)

European Commission [EC]. (s.f.). *Payment services*.  
<https://ec.europa.eu/newsroom/fisma/items/658958>

European Investment Bank [EIB]. (2021). *EIB issues its first ever digital bond on a public blockchain*. <https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain>

European Parliament [EP]. (2022). *Revision of the eIDAS Regulation*.

European Securities and Markets Authority [ESMA]. (2012). *MiFID Questions and Answers. Investor protection and intermediaries*. ESMA.

European Securities and Markets Authority [ESMA]. (2014). *MiFID practices for firms selling complex products*. ESMA/2014/146.

Financial Conduct Authority [FCA]. (2021a). *Green FinTech Challenge 2021*.  
<https://www.fca.org.uk/firms/innovation/green-FinTech-challenge>

Financial Conduct Authority [FCA]. (2021b). *Open finance*. Feedback Statement.

Financial Conduct Authority [FCA]. (2022a). *Insights from our Approach to Regulatory Innovation. RegTech Forum – Approach to Regulatory Innovation & SupTech*.  
<https://www.fca.org.uk/events/RegTech-forum-fca-approach-innovation-SupTech>

Finezza. (2020). *Home*. <https://finezza.in/blog/faas-the-emerging-global-trend-of-FinTech-as-a-service/>

Finreg 360. (2022). *La ESMA consulta sobre las normas de transparencia y «reporting» del régimen piloto de las infraestructuras de mercado basadas en DLT*.  
<https://finreg360.com/alerta/la-esma-consulta-sobre-las-normas-de-transparencia-y-reporting-del-regimen-piloto-de-las-infraestructuras-de-mercado-basadas-en-registro-descentralizado/>

*FinTech Finance*. (2019). *Revolut launches Silver and Space Grey metal card colours*. <https://www.FinTechf.com/01-news/revolut-launches-silver-and-space-grey-metal-card-colours/>

Frey, C., & Presidente, G. (2022). *The GDPR effect: How data privacy regulation shaped firm performance globally*. <https://voxeu.org/article/how-data-privacy-regulation-shaped-firm-performance-globally>

Fxempire. (2018). *What are ILP's (Initial Loan Procurements) and How Does it Work?* <https://www.fxempire.com/education/article/what-are-ilps-initial-loan-procurements-and-how-does-it-work-517180>

García, A., & Natalucci, F. (2022). *Fast-Moving FinTech Poses Challenge for Regulators*. IMF Blog: <https://blogs.imf.org/2022/04/13/fast-moving-FinTech-poses-challenge-for-regulators/#>

Gensler, G. (2019). *Examining Facebook's proposed cryptocurrency and its impact on consumers, investors, and the American Financial Systems*. Financial Services Committee. United States House of Representatives.

González, J. (2022). *De la identidad a la identidad digital soberana. Los servicios electrónicos de confianza y seguridad jurídica*. <https://tallerdederechos.com/de-la-identidad-a-la-identidad-digital-soberana/>

Gorjón, S. (2021). *Plataformas digitales y servicios financieros. Congreso Jurídico Internacional sobre Plataformas Digitales*. <https://agenda.uib.es/57847/section/28444/congreso-juridico-internacional-sobre-plataformas-digitales.html>

Groß, J., Schiller, J., & Sandner, P. (2019). *Facebook-coin Libra: benefits vs. risks — opinions from German economists*. Frankfurt School of Finance & Management: <https://philippsandner.medium.com/facebook-coin-libra-benefits-vs-risks-insights-from-german-economists-2707b2c316fb>

Guerrera, E. (2022). *La sentencia que mantiene al desarrollador de Tornado Cash en la cárcel durante 90 días provoca una reacción violenta*. Cointelegraph: <https://es.cointelegraph.com/news/ruling-to-keep-tornado-cash-developer-in-jail-for-90-days-sparks-backlash>

Hammer, S. (2021). *Cryptocurrency and Blockchain: an Introduction to Digital Currencies*. University of Pennsylvania Law School.

Hauptman, M., Morris, N., Uribe, J., Goyal, D., Batra, I., & Rakhimova, K. (2022). *White paper. Matchmaker, Make Me a Match. Best practices in bank-FinTech partnerships*. Boston Consulting Group.

Howe, J. (2006). The rise of crowdsourcing. *Wired magazine*, 14(6), 1-4. <https://www.wired.com/2006/06/crowds/>

Hoyler, E. (2022). *Adopting the principle of "same activity, same risk, same regulation" into the UK's regulatory framework*. <https://www.ukfinance.org.uk/news-and-insight/blogs/adopting-principle-uks-regulatory-framework>

Idaho Department of Finance. (2020). *Initial Loan Procurements*. <https://www.finance.idaho.gov/about/press-releases/documents/2020/2020-pr-initial-loan-procurement.pdf>

Infopulse. (2019). *Introducing Super App: a New Approach to All-in-One Experience*. [https://medium.com/@infopulseglobal\\_9037/introducing-super-app-a-new-approach-to-all-in-one-experience-8a7894e8ddd4](https://medium.com/@infopulseglobal_9037/introducing-super-app-a-new-approach-to-all-in-one-experience-8a7894e8ddd4)

International Capital Markets Association [ICMA]. (2022). *ICMA response to ESMA call for evidence on the DLT pilot regime*. ICMA.

International Token Standardization Association. (2019). *Setting standards for global token markets*. [https://www.bvi.de/fileadmin/user\\_upload/Regulierung/Branchenstandards/20190125\\_-\\_ITSA\\_-\\_Setting\\_Standards\\_for\\_Global-Token\\_Markets.pdf](https://www.bvi.de/fileadmin/user_upload/Regulierung/Branchenstandards/20190125_-_ITSA_-_Setting_Standards_for_Global-Token_Markets.pdf)

J.P. Morgan. (2022). *White paper. ISO 20022—El lenguaje universal para el futuro de pagos*. <https://www.jpmorgan.com/content/dam/jpm/global/documents/iso-20022-spanish-white-paper-ada-compliant.pdf>

Jenkinson, G. (2022). *Un NFT de CryptoPunk se dividirá en miles de piezas*. Cointelegraph: <https://es.cointelegraph.com/news/a-slice-of-the-punk-cryptopunk-nft-to-be-split-into-56-000-pieces>

Jennings, M. (2022). *Principles & Models of Web3 Decentralization*. [https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralization\\_miles-jennings\\_a16zcrypto.pdf](https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf)

Jin, L.-j., Vijay, M., & Akhil, S. (2002). *Analysis on Service Level Agreement of Web Services*. HP Laboratories Palo Alto: <https://www.hpl.hp.com/techreports/2002/HPL-2002-180.pdf>

John, A. (2020). *Explainer: How does China's digital yuan work?* Reuters: <https://www.reuters.com/article/us-china-currency-digital-explainer-idUSKBN27411T>

Johnson, S. (2022). *Set to mandate PSD3 API standardization*. Business News: <https://biz.crastr.net/set-to-mandate-psd3-api-standardization/>

Johnston, D., Yilmaz, S., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., Mason, S. (2020). *The General Theory of Decentralized Applications, Dapps*. <https://github.com/DavidJohnstonCEO/DecentralizedApplications>

Jones, M. (2021). *Digital euro might suck away 8% of banks' deposits -Morgan Stanley*. Reuters: <https://www.reuters.com/business/finance/digital-euro-might-suck-away-8-banks-deposits-morgan-stanley-2021-06-15/>

Kahn, L. M. (2017). Amazon's antitrust paradox. *The Yale Law Journal* 126, 710 (pp.710-805). [https://www.yalelawjournal.org/pdf/e.710.Khan.805\\_zuvfyyeh.pdf](https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf)

Karp, H., & Melbardis, R. (2021). *Nexus Mutual*. [https://nexusmutual.io/assets/docs/nmx\\_white\\_paperv2\\_3.pdf](https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf)

Klein, M. (2021). *How can Commercial Banks Provide a DLT Based Retail-Euro?* <https://docs.google.com/document/d/1fFU8DrnkVm0zdMsPwmE13hfbHBrVpKxj1E-Mn4ABQmo/edit>

KPMG. (2022). *The collapse of FTX*. KPMG.

Kremers, J., Schoenmaker, D., & Wierts, P. (2003). *Financial Supervision in Europe*. Ministry of Finance Netherlands.

Lagerwaard, P. (2018). *Following Suspicious Transactions in Europe*. [http://www.projectfollow.org/wp-content/uploads/2017/07/Research\\_Report\\_2018\\_Lagerwaard.pdf](http://www.projectfollow.org/wp-content/uploads/2017/07/Research_Report_2018_Lagerwaard.pdf)

Larrauri, J. (2022). *Nos vamos a un mundo de Super Apps y nosotros sin saberlo*. [https://www.linkedin.com/pulse/nos-vamos-un-mundo-de-super-apps-y-nosotros-sin-saberlo-juan-larrauri/?trk=public\\_post\\_main-feed-card\\_feed-article-content](https://www.linkedin.com/pulse/nos-vamos-un-mundo-de-super-apps-y-nosotros-sin-saberlo-juan-larrauri/?trk=public_post_main-feed-card_feed-article-content)

Lau, D., Lau, D., Jin, T., Kho, K., Azmi, E., Lee, T., & Ong, B. (2020). *How to Defi*. CoinGecko.

Lautenschläger, S. (2017). *Digital native FinTechs and the future of banking*. European Central Bank: [https://www.bankingsupervision.europa.eu/press/speeches/date/2017/html/se170327\\_1.en.html](https://www.bankingsupervision.europa.eu/press/speeches/date/2017/html/se170327_1.en.html)

Lawrence, K. (2013). *Developing leaders in a VUCA environment*. <https://www.emergingrleader.com/wp-content/uploads/2013/02/developing-leaders-in-a-vuca-environment.pdf>

Legal nodes. (2020). *Figure out the legal wrapper for your DAO*. <https://legalnodes.com/product/dao-legal-wrapper>

Libra Association. (2020). *Libra White Paper v.2.0*. Diem: <https://www.diem.com/en-us/white-paper/>

Llaneza González, P. (2022). La identidad digital, el cambio de modelo de eIDAS a eIDAS 2. *Los servicios electrónicos de confianza y seguridad jurídica*. [https://tv.comillas.edu/media/Los+servicios+electr%C3%B3nicos+de+confianza+y+la+seguridad+jur%C3%ADdica.+Del+Reglamento+eIDAS+y+la+Ley+6+2020+a+la+propuesta+de+eIDAS2.+1%C2%BA+Sesi%C3%B3n+Ma%C3%B1ana.+++10+02+2022/1\\_7j0utqgp](https://tv.comillas.edu/media/Los+servicios+electr%C3%B3nicos+de+confianza+y+la+seguridad+jur%C3%ADdica.+Del+Reglamento+eIDAS+y+la+Ley+6+2020+a+la+propuesta+de+eIDAS2.+1%C2%BA+Sesi%C3%B3n+Ma%C3%B1ana.+++10+02+2022/1_7j0utqgp)

London Stock Exchange Group [LSEG]. (2021). *LSEG position paper on European commission's Digital Operational Resilience Act (DORA)*.

Marcus, D. (2019). *Hearing Before the United States House of Representatives Committee on Financial Services*. <https://financialservices.house.gov/uploadedfiles/hhr-116-ba00-wstate-marcusd-20190717.pdf>

Martínez, J. A. (2021). *Encuentro con el sector sobre FinTech y Seguridad*. CNMV: <https://www.cnmv.es/Portal/FinTech/Jornadas.aspx>

Matcha. (s.f.). *Home*. <https://matcha.xyz/>

McKee, J. (2020). *Embedded Finance: A Beginner's Guide To The Growing Intersection of Tech and Financial Services*. Forbes: <https://www.forbes.com/sites/jordanmckee/2020/12/16/embedded-finance-a-beginners-guide-to-the-growing-intersection-of-tech-and-financial-services/?sh=56b827e924af>

Meegan, X., & Koens, T. (2021). *Lessons Learned from Decentralised Finance (DeFi)*. [https://new.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi\\_white\\_paper\\_v2.0.pdf](https://new.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2.0.pdf)

Mercado Libre. (2021). *Home*. <https://investor.mercadolibre.com/>

Microsoft. (2021). *Microsoft response to the European Commissions proposal for a regulation on digital operational resilience for the financial services sector*.

Ministerio de Justicia. (2021). *Registradores de España*.  
<https://www.justicia.lei.registradores.org/?AspxAutoDetectCookieSupport=1#:~:text=El%20Identificador%20de%20Entidad%20Jur%C3%ADdica,informaci%C3%B3n%20en%20los%20mercados%20financieros>.

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. (2021). *Carta de derechos digitales*.  
[https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta\\_Derechos\\_Digitales\\_RedEs.pdf](https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf)

Mirza, J. (2022). *Ethereum Merge Date: When Is The Ethereum Merge?* Planet Crypto:  
<https://www.gfinityesports.com/cryptocurrency/ethereum-merge-date/>

Mohanti, D. (2019). *Ripple and Stablecoins. Building Banks of Tomorrow*. Publications India.

Muhn, J. (2021). *25 FinTechs going green*. Finovate: <https://finovate.com/20-FinTechs-going-green/>

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.  
<https://bitcoin.org/bitcoin.pdf>

Neward, B. (2022). *Última hora: El puente Horizon de Harmony ha sido hackeado por 100 millones de dólares*. Cointelegraph: <https://es.cointelegraph.com/news/breaking-harmony-one-s-horizon-bridge-hacked-for-100m>

Open Banking Brasil. (2021). *Conheça o Open Banking*.  
<https://openbankingbrasil.org.br/conheca/?cookie=true>

ORACLE. (2021). *SWIFT Integration Projects*. SWIFT Message Type Reference:  
<https://docs.oracle.com/cd/E19509-01/820-7113/6nid5dl2r/index.html>

Ordóñez, M. A. (2021). *El Euro digital nos interesa*. Madrid Digital Coin Summit.

Organización de Consumidores y Usuarios [OCU]. (2022). *Códigos QR: qué son y para qué sirven*. <https://www.ocu.org/tecnologia/telefono/noticias/codigos-qr-que-son-y-para-que-sirven576294>

Ortiz, A. M. L. (2017). *La actividad pública de supervisión bancaria. Reforma y responsabilidad de la administración*. Universitat Jaume I:  
[https://www.tdx.cat/bitstream/handle/10803/404532/2017\\_Tesis\\_Lara%20Ortiz\\_MariaLidon.pdf?sequence=1](https://www.tdx.cat/bitstream/handle/10803/404532/2017_Tesis_Lara%20Ortiz_MariaLidon.pdf?sequence=1)

Pancake Swap. (2022). *IFO (Initial Farm Offering)*.  
<https://docs.pancakeswap.finance/products/ifo-initial-farm-offering>

Panetta, F. (2020). *The two sides of the (stable)coin*. European Central Bank: <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201104~7908460f0d.en.html>

Perc, P., & Forst, F. (2017). *Towards Banking as a service. Cloud-based service models and the transformation of banking*. [https://zeb-consulting.com/files/media/documents/2019-11/zeb\\_Topic\\_%20Towards%20banking\\_as\\_a\\_service\\_2018\\_EN.pdf](https://zeb-consulting.com/files/media/documents/2019-11/zeb_Topic_%20Towards%20banking_as_a_service_2018_EN.pdf)

Peterson, J., Krug, J., Zoltu, M., Williams, A., & Alexander, S. (2021). *Augur: a Decentralized Oracle and Prediction Market Platform (v2.0)*. <https://github.com/AugurProject/whitepaper>

Pradel, L., & Hochedez, A. (2022). *Millennials and banks : how to develop a winning customer relationship*. <https://worldline.com/en/home/knowledgehub/blog/2022/january/millennials-and-banks-how-to-develop-a-winning-customer-relationship.html>

Pryor, R. (2022). *NFTs recognised as 'legal property' in landmark case*. The Art Newspaper: <https://www.theartnewspaper.com/2022/04/29/nfts-recognised-as-legal-property-in-landmark-case>

Reul, F., Bruemjes, T., Ketz, C., Wurzel, R., & Labetzsch, C. (2022). Industry Insights (CAC22A) – Implementing Digital Asset Infrastructure. *Crypto Assets Conference*. Frankfurt School Blockchain Center.

Reuters. (2018). *ECB has no plan to issue digital currency: Draghi*. <https://www.reuters.com/article/us-ecb-bitcoin-idUSKCN1LU1JM>

Roosevelt, F. D. (27 de junio de 1936). *Acceptance Speech for the Renomination for the Presidency, Philadelphia, Pa.* The American Presidency Project: <https://www.presidency.ucsb.edu/>

Sablier. (2021). *Home*. <https://sablier.finance/>

Sandner, P., Ferreira, A., Gross, J., Katilmis, S., & Forster, M. (20 de June de 2022). *Circle's New Euro Stablecoin: Issued from the US and Used Outside the EU?* <https://philippsandner.medium.com/circles-new-euro-stablecoin-issued-from-the-us-and-used-outside-the-eu-b1d3fa2a4432>

Sarin, N. (2020). *FinTech: Overview, Payments and Regulation*. <https://www.coursera.org/learn/wharton-FinTech-overview-payments-regulations>

Schickler, J. (2022). *Alexey Pertsev, desarrollador de Tornado Cash, seguirá en prisión hasta al menos fines de febrero*. <https://www.coindesk.com/es/policy/2022/11/22/alexey-pertsev-desarrollador-de-tornado-cash-seguira-en-prision-hasta-al-menos-fines-de-febrero/>

Security Standards Council [PCI]. (2018). *Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures*. [https://www.pcisecuritystandards.org/pdfs/pci\\_ssc\\_quick\\_guide.pdf](https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf)

Segal-Knowles, C. (2021). *Stablecoins: what's old is new again*. Westminster eForum Policy Conference. Bank of England: <https://www.bankofengland.co.uk/speech/2021/june/christina-segal-knowles-speech-at-the-westminster-eforum-poicy-conference>

Shen, M. (2022). *How \$60 Billion in Terra Coins Went Up in Algorithmic Smoke*. <https://www.bloomberg.com/graphics/2022-crypto-luna-terra-stablecoin-explainer/>

Shepherd-Barron, J. (2017). *Meet the true star of financial innovation — the humble ATM*. Financial Times: <https://www.ft.com/content/052f9310-5738-11e7-80b6-9bfa4c1f83d2>

Snapshot Labs. (2022). *Snapshot*. <https://snapshot.org/#/>

Solarisbank A.G. (2020). *Solarisbank newsroom*. <https://solarisbank.pr.co/191900-solarisbank-partners-with-samsung-electronics-and-visa-to-launch-samsung-pay-in-germany>

Solarisbank A.G. (2019). *Solarisbank newsroom*. <https://solarisbank.pr.co/171960-solarisbank-becomes-alipay-s-acquirer-for-further-merchant-network-expansion-in-europe>

Soon, T. J. (2008). *QR Code*. [https://foxdesignstudio.com/uploads/pdf/Three\\_QR\\_Code.pdf](https://foxdesignstudio.com/uploads/pdf/Three_QR_Code.pdf)

Staschen, S., & Meagher, P. (2022b). *Platform-Based Finance: How Can Regulators Preserve Competition?* Consultative Group to Assist the Poor [CGAP]: <https://www.cgap.org/blog/platform-based-finance-how-can-regulators-preserve-competition>

Stauber, P. (2019). Facebook's abuse investigation in Germany and some thoughts on cooperation between anti-trust and data protection authorities. *CPI Antitrust Chronicle*. [https://noerr.com/Mailings/Kartellrecht/Brussels%20Matters%202019\\_04\\_11/CPI\\_Facebook%20investigation\\_Stauber.pdf](https://noerr.com/Mailings/Kartellrecht/Brussels%20Matters%202019_04_11/CPI_Facebook%20investigation_Stauber.pdf)



SWIFT. (2016). *RMA and RMA Plus: managing your correspondent connections*.  
file:///C:/Users/ayalg/Downloads/swift\_compliance\_infopaper\_rma.pdf

SWIFT. (2021). *ISO 20022 adoption programme*. <https://www.swift.com/standards/iso-20022/iso-20022-programme/timeline>

SWIFT. (2022a). *An update to our message for the SWIFT Community*.  
<https://www.swift.com/news-events/news/message-swift-community>

SWIFT. (2022b). *SWIFT history*. <https://www.swift.com/es/node/10436>

Takahashi, M. (2021). *Hashtack Finance. Non-custodial, DeFi's only under-collateralised lending protocol enabling 3x loans to collateral*.  
<https://hackernoon.com/hashstack-is-bringing-under-collateralized-loans-to-crypto-lending>

Tapia, A. (2021b). *Sostenibilidad y digitalización en el mercado de seguros: Temas centrales del Informe anual 2020 de EIOPA*. El Blog de Alberto J. Tapia Hermida:  
<http://ajtapia.com/2021/07/sostenibilidad-y-digitalizacion-en-el-mercado-de-seguros-temas-centrales-del-informe-anual-2020-de-eiopa/>

Teslafan. (2021). *Whitepaper 1.0*. <https://teslafantoken.gitbook.io/white-paper/contents/v1.0>

The CityUK. (2021). *Cryptoassets: Shaping UK regulation for innovation and global leadership*. <https://www.thecityuk.com/research/cryptoassets-shaping-uk-regulation-for-innovation-and-global-leadership/>

Theiyeer Report. (2022). *A brief timeline of FinTech*. <http://www.theiyeerreport.com/wp-content/uploads/2017/07/A-Brief-Timeline-of-FinTech.pdf>

UK HM Treasury. (2022). *UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence*. UK HM Treasury.

University of Nicosia. (2022). *Bitcoin clients, online wallets, cold storage, sending, & receiving. DFIN 511: Introduction to Digital Currencies*.

Unnax Regulatory Services, EDE, S.L. (2020). *Home*.  
<https://www.unnax.com/?lang=es>

Unnax. (2020). *The future of Banking as a Service (BaaS)*.  
<https://cdn2.hubspot.net/hubfs/2535354/ebooks/ebook%20The%20future%20of%20banking%20as%20a%20service,%20BaaS.pdf>

von der Leyen, U. (2019). *Executive Vice-President-designate for An Economy that Works for People*. [https://ec.europa.eu/info/sites/default/files/mission-letter-valdis-dombrovskis-2019\\_en.pdf](https://ec.europa.eu/info/sites/default/files/mission-letter-valdis-dombrovskis-2019_en.pdf)

Westlaw. (2020). *¿Qué es un iniciador de pagos y cuáles son sus requisitos?* <https://letslaw.es/iniciador-de-pagos/>

Willson, T. (2022). *Reuters european markets. Rouble-crypto trading soars as sanctions hit Russian currency*. <https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/>

Wittayatanaseth, N. (2018). *Stablecoins: De-Risking Non-Collateralized Stablecoins*. <https://medium.com/@natwittayatanaseth/https-medium-com-FinTech-kellogg-de-risking-non-collateralized-stablecoins-40e832562090>

Wolfsberg Group. (2020). *Banca Corresponsal. Cuestionario de Diligencia Debida. Guía de cumplimentación*. [https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%27s\\_CBDDQ\\_Gu%C3%ADa%20de%20Cumplimentaci%C3%B3n\\_Spanish%20%28final%29.pdf](https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%27s_CBDDQ_Gu%C3%ADa%20de%20Cumplimentaci%C3%B3n_Spanish%20%28final%29.pdf)

Wood, G. (2016). *Polkadot: vision for a heterogeneous multi-chain framework*. <https://polkadot.network/PolkaDotPaper.pdf>

Wuermeling, J. (2021, September 23). *Exploring DORA - the Digital Operational Resilience Act and its impact on banks and their supervisors*. Deutsche Bundesbank. <https://www.bundesbank.de/en/press/speeches/exploring-dora-the-digital-operational-resilience-act-and-its-impact-on-banks-and-their-supervisors-876006>

Wuermeling, J. (2022, June 2). *Regulating innovation or innovating regulation? What it takes to make digital finance a success*. Deutsche Bundesbank. <https://www.bundesbank.de/en/press/speeches/regulating-innovation-or-innovating-regulation-what-it-takes-to-make-digital-finance-a-success-892016>

Zhang, S., & Ruwitch, J. (2021). *Exclusive: Ant Financial shifts focus from finance to tech services*. <https://www.reuters.com/article/us-china-ant-financial-regulation-exclus-idUSKCN1J10WV>

## **Normativa española**

Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión.

Circular 4/2020, de 26 de junio, del Banco de España, sobre publicidad de los productos y servicios bancarios.

Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. *BOE núm. 156.*

Ley 16/2011, de 24 de junio, de contratos de crédito al consumo. *BOE núm. 151.*

Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. *BOE núm. 168*

Ley 21/2007, de 11 de julio, por la que se modifica el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, y el texto refundido de la Ley de ordenación y supervisión de los seguros privados, aprobado por el Real Decreto Legislativo 6/2004, de 29 de octubre. *BOE núm. 166*

Ley 21/2011, de 26 de julio, de dinero electrónico. *BOE núm. 171.*

Ley 27/1999, de 16 de julio, de Cooperativas. *BOE núm. 170.*

Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones. *BOE núm. 303.*

Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre. *BOE núm. 76.*

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial. (2015). *BOE núm. 101.*

Ministerio de Gracia y Justicia. (1889). *Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.* <https://boe.gob.es/buscar/act.php?id=BOE-A-1889-4763&p=20210605&tn=0>

Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Real Decreto 736/2019, de 20 de diciembre, de régimen jurídico de los servicios de pago y de las entidades de pago y por el que se modifican el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico, y el Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito

Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico.

Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores.

Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

## **Normativa europea**

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax

Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (versión refundida) (Texto pertinente a efectos del EEE).

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se der. (25 de noviembre de 2015).

Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (Texto pertinente a efectos del EEE)

Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo de 20 de enero de 2016 sobre la distribución de seguros (versión refundida) (Texto pertinente a efectos del EEE).

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n° 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos

Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE (Texto pertinente a efectos del EEE).

Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo.

Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifi.

Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) N.º 1060/2009 y (UE) N.º 1095/2010 Texto pertinente a efectos del EEE.

Directiva 2014/57/UE del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre las sanciones penales aplicables al abuso de mercado (Directiva sobre abuso de mercado)

Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (refundición) (Texto pertinente a efectos del EEE).

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives.

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

European Banking Authority [EBA]. (2017c). *Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)*. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

European Banking Authority [EBA]. (2019a). *EBA Guidelines on outsourcing arrangements*. *EBA/GL/2019/02*. <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements#:~:text=The%20EBA%20Guidelines%20will%20enter,other%20service%20providers%2C%20if%20the>

European Central Bank [ECB]. (2014). *Guide to Banking Supervision*. European Central Bank (ECB).

European Commission [EC]. (2020a). *Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC* COM/2020/825 final. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>

European Commission [EC]. (2020b). *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)* COM (2020) 842 final. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>

European Commission [EC]. (2020d). *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*. Unión Europea. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

European Commission [EC]. (2020e). *Proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595>

European Commission [EC]. (2021c). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. COM (2021) 281 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>

European Commission [EC]. (2021e). *Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)*. [https://ec.europa.eu/finance/docs/law/210720-proposal-funds-transfers\\_en.pdf](https://ec.europa.eu/finance/docs/law/210720-proposal-funds-transfers_en.pdf)

European Data Protection Board. (2021). *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR. Version 2.0*. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en)

European Parliament [EP]. (2023, May 31). *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives*

2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

European Parliament [EP]. (2014, July 23). Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 in improving securities settlement in the European Union and on central securities depositories and amending Directives 98/23/EC and Regulation (EU) N° 236/2012. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0909>

European Parliament [EP]. (2019). *Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0876>

European Parliament [EP]. (2022a). *Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0858>

Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo de 14 de junio de 2017 sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE (Texto pertinente a efectos del EEE)

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011 (Texto pertinente a efectos del EEE)

Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.



Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937. Reglamento (UE) N.º 600/2014 del Parlamento Europeo y del Consejo del 15 de mayo de 2014 relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) no 648/2012 (Texto pertinente a efectos del EEE).

Reglamento de Ejecución (UE) 2017/1469 de la Comisión de 11 de agosto de 2017 por el que se establece un formato de presentación normalizado para el documento de información sobre productos de seguro (Texto pertinente a efectos del EEE)

Reglamento Delegado (UE) 2017/2358 de la Comisión de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de control y gobernanza de los productos aplicables a las empresas de seguros y los distribuidores de seguros (Texto pertinente a efectos del EEE).

Reglamento Delegado (UE) 2017/2359 de la Comisión de 21 de septiembre de 2017 por el que se completa la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de información y las normas de conducta aplicables a la distribución de productos de inversión basados en seguros (Texto pertinente a efectos del EEE).

Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada. (s.f.).

Reglamento UE N° 596/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión (Texto pertinente a efectos del EEE)

Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013. (s.f.).

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology,

and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65.

Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 in improving securities settlement in the European Union and on central securities depositories and amending Directives 98/23/EC and Regulation (EU) N° 236/2012. (s.f.).

## Otra Normativa de referencia

Congress.gov. (2021, March 8). *H.R.1628 - Token Taxonomy Act of 2021*. <https://www.congress.gov/bill/117th-congress/house-bill/1628/text>. Estados Unidos.

Congress.gov. (2022). *S.4356 - Lummis-Gillibrand responsible financial innovation act*. <https://www.congress.gov/bill/117th-congress/senate-bill/4356>. Estados Unidos.

Disposiciones de carácter general relativas a las interfaces de programación de aplicaciones informáticas estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera publicada en el DOF el 4 de junio de 2020. Mexico.

Financial Conduct Authority [FCA]. (2022b). *UK FCA Handbook*. <https://www.handbook.fca.org.uk/handbook> Reino Unido.

Govern d'Andorra. (2022). *Llei 24/2022, del 30 de juny, de la representació digital d'actius mitjançant l'ús de la criptografia i de la tecnologia de llibre registre distribuït i blockchain*. [https://www.bopa.ad/bopa/034086/Pagines/CGL20220715\\_13\\_23\\_43.aspx](https://www.bopa.ad/bopa/034086/Pagines/CGL20220715_13_23_43.aspx). Andorra.

Ley para Regular las Instituciones de Tecnología Financiera se publicó en el Diario Oficial de la Federación (DOF) el 9 de marzo de 2018. Mexico.

Llei 24/2022, del 30 de juny, de la representació digital d'actius mitjançant l'ús de la criptografia i de la tecnologia de llibre registre distribuït i blockchain . (30 de June de 2022). Andorra.

Lummis, S. (2022). *S.4356 - Lummis-Gillibrand Responsible Financial Innovation Act*. Senate and House of Representatives of the United States of America. (2019). *Discussion draft to prohibit large platform utilities from being a financial institution or being affiliated with a person that is a financial institution, and for other purposes*. [https://financialservices.house.gov/uploadedfiles/bills-116hr\\_\\_\\_\\_ih-BigTech.pdf](https://financialservices.house.gov/uploadedfiles/bills-116hr____ih-BigTech.pdf)

White House. (2022). *Executive Order on Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine*. Briefing room: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/02/21/executive-order-on-blocking-property-of-certain-persons-and-prohibiting-certain-transactions-with-respect-to-continued-russian-efforts-to-undermine-the-sovereignty-and-territorial-integrity-of-ukraine/>. Estados Unidos.

## Doctrina y jurisprudencia

Commission Decision of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)), AT.39740 (European Commission 26 de June de 2017).

Court of Justice of the European Union. (2015, October 22). *Judgment of the Court of Justice of the European Union (Fifth Chamber) 22 October 2015 (Reference for a preliminary ruling — Common system of value added tax (VAT) — Directive 2006/112/EC — Articles 2(1)(c) and 135(1)(d) to (f) — Services for consideration, C-264/14.*

<https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EN>

Court of Justice of the European Union. (2018, December 3). *Judgment of the Court (Fifth Chamber) of 4 October 2018 (request for a preliminary ruling from the Oberster Gerichtshof — Austria) — Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG, Case C-191/17.* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CA0191>

Denuncia en Primera Instancia Juzgado de lo Mercantil Bilbao núm. 2, S 24-07-2015, nº 197/2015, rec. 199/2015, nº autos 199/2015, 197/2015 (Juzgado de lo Mercantil Bilbao núm. 2 24 de julio de 2015).

DGT, Consulta nº V4050/2015 del 16 de diciembre de 2015, V4050/2015 (Dirección General de Tributos 16 de diciembre de 2015).

DGT, Resolución Vinculante de Dirección General de Tributos, V0486-22 de 10 de Marzo de 2022

DGT, Resolución Vinculante de Dirección General de Tributos, V2107-18 de 17 de Julio de 2018

European Parliament [EP]. (2016). *European Parliament resolution on virtual currencies (2016/2007 (INI)), 2016/2007 (INI).* [https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_EN.html)

European Parliament [EP]. (2017). *Sentencia del Tribunal de Justicia (Gran Sala) de 20 de diciembre de 2017. Asociación Profesional Élite Taxi contra Uber Systems Spain, SL., Asunto C-434/15.* <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A62015CJ0434>

Landgericht Ravensburg. (2021). *Request for a preliminary ruling from the Landgericht Ravensburg (Germany) lodged on 22 January 2021 – VK v BMW Bank GmbH (Case C-38/21)*.

<https://curia.europa.eu/juris/document/document.jsf?jsessionid=5CE63E37EE411267CB8E61F075267C80?text=&docid=239701&pageIndex=0&doclang=en&mode=doc&dir=&occ=first&cid=11696463>

Louis K. Liggett Co. v. Lee, 288 U.S. 517, 53 S. Ct. 481, 77 L. Ed. 929, 85 A.L.R. 699 (U.S. Mar. 13, 1933).

Nessa Risley vs Universal Navigation Inc. dba Uniswap Labs, 1:22 (United States District Court Southern District of New York 4 de abril de 2022).

<https://www.classaction.org/media/risley-v-universal-navigation-inc-et-al.pdf>

Recurso de Apelación AP Asturias, sec. 4ª, S 06-02-2015, nº 37/2015, rec. 27/2015, 37/2015 (Audiencia Provincial de Asturias 6 de febrero de 2015).

SEC vs Ishan Wahi, Nikhil Wahi, and Sameer Ramani, Case 2:22-cv-01009 (21 de July de 2022).

SEC vs Poloniex, LLC, 3-20455 (Securities Exchange Commission (SEC) 9 de August de 2021). <https://www.sec.gov/litigation/admin/2021/34-92607.pdf>

Secretaría de Estado de Hacienda. Dirección General de Tributos. (2021). *Doctrina tributaria. Consultas tributarias.*

[https://petete.tributos.hacienda.gob.es/consultas/?num\\_consulta=V2679-21](https://petete.tributos.hacienda.gob.es/consultas/?num_consulta=V2679-21)

Sentencia del Tribunal de Justicia (Gran Sala) de 20 de diciembre de 2017. Asociación Profesional Élite Taxi contra Uber Systems Spain, SL., Asunto C-434/15 (Tribunal de Justicia de la Unión Europea 20 de diciembre de 2017).

Sentencia del Tribunal de Justicia (Sala Quinta) de 22 de octubre de 2015 «Procedimiento prejudicial — Sistema común del impuesto sobre el valor añadido (IVA) — Directiva 2006/112/CE — Artículos 2, apartado 1, letra c), y 135, apartado 1, letras d) a f) — Servicios a título oneroso — Operaciones de cambio de la divisa virtual “bitcoin” por divisas tradicionales — Exención» Asunto C-264/14

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª) número 326/2019, de 20 de junio. (2019).

Skatteverket v Hedqvist, Celex No. 62014CJ0264 (Tribunal de Justicia de la Unión Europea 22 de Octubre de 2015).

United States District Court Southern District of New York. (2022, April 4). *Nessa Risley vs Universal Navigation Inc. dba Uniswap Labs*, 1:22. <https://www.classaction.org/media/risley-v-universal-navigation-inc-et-al.pdf>

United States District Court Western District of Washington Seattle Division. (2022, July 21). *SEC vs Ishan Wahi, Nikhil Wahi, and Sameer Ramani, Case 2:22-cv-01009*. <https://www.sec.gov/litigation/complaints/2022/comp-pr2022-127.pdf>