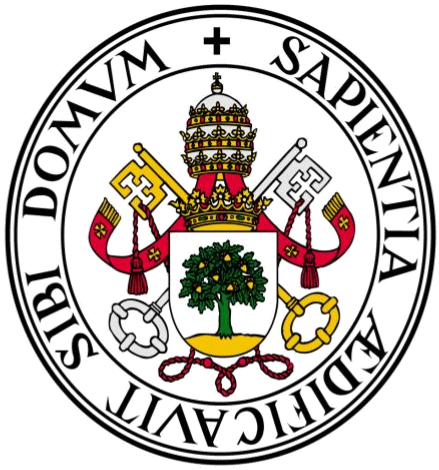

Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

La custodia de los criptoactivos en el reglamento MiCA

Presentado por:

David Charpentier Rodríguez

Tutelado por:

Javier Damaso Vicente Blanco

Valladolid, 3 de Marzo de 2025

ÍNDICE

Resumen

El objetivo principal del presente trabajo es el análisis basado en la necesidad de implementar el Reglamento MiCA y se complementa con la importancia del custodio de los criptoactivos, clave en el futuro de los aspectos tecnológicos a tratar, a través de la normativa regulatoria a nivel europeo sobre los mercados de criptoactivos.

En primer lugar, nos muestra el avance incipiente que se está produciendo en este sector y la transición que se ha ido produciendo para adaptarse a las nuevas realidades del mercado, respecto a MiFID como precedente, para garantizar seguridad y protección a los consumidores, de tal forma, que los proveedores de servicios de criptoactivos puedan operar con mayor facilidad en todos los mercados de la UE, en virtud de, un marco regulatorio único.

Palabras clave: Reglamento Mica, criptoactivos, custodia, proveedores de servicios.

Abstract

The main objective of this work is to analyze the need for the implementation of the MiCA Regulation, complemented by the importance of crypto asset custodians, which are key to addressing future technological aspects, through the European regulatory framework for crypto asset markets.

Firstly, it highlights the emerging progress taking place in this sector and the transition that has occurred to adapt to the new market realities, referencing MiFID as a precedent, to ensure consumer safety and protection. This ensures that crypto asset service providers can operate more easily across all EU markets under a unified regulatory framework.

Keywords: MiCA Regulation, crypto-assets, custody, service providers.

Ámbito de trabajo e importancia

El campo de investigación el cual se orienta el trabajo esta relación con todo lo referente a los criptoactivos en el ámbito internacional, el gran peso que tienen actualmente y como han ido evolucionando en una sociedad cada vez más propensa a las nuevas tecnologías. Para iniciar el tema, consta del gran significado que representa el Reglamento

MiCA a nivel europeo como concepto crucial para entender todo lo que procede, y MiFID para entender de dónde precede

Ante los casos de fraudes y fallos de gran escala que se ha producido a lo largo de la historia, veremos la necesidad de recurrir a los custodios de los criptoactivos, como aspecto clave en hacer hincapié del presente trabajo. Tanto en el pasado, como en el presente y futuro, el dinero, no dejara de ser nunca objeto de preocupación para las personas, debido a la importancia que conlleva sentir seguridad en tener a salvo los ahorros y confianza para operar en el mercado.

Objetivos del análisis.

Los objetivos a los que trataremos de buscar respuesta:

- Estudio del contenido del Reglamento MiCA desde su necesidad, evolución y lo que pretende.
- La custodia de los criptoactivos como pilar clave en el reglamento, el modelo de custodio empleado y la resiliencia de los activos.

Metodología aplicada.

La parte teórica del trabajo incluye los dos primeros capítulos, en los cuales, hemos recopilado información de diferentes libros, manuales, guías y diferentes blogs.

La parte jurídica hace referencia al tercer capítulo, donde se reflejará los artículos del reglamento MiCA, en relación con el custodio de los criptoactivos publicados en el BOE y en el Reglamento de la UE.

Estructura del trabajo.

La estructura que contiene este Trabajo de Fin de Grado es la siguiente:
En primer lugar, nos centramos en los dos primeros capítulos de carácter teórico, desde una perspectiva histórica sobre la delimitación del MIFID II hasta la necesidad de implementar el Reglamento MiCA, como su importancia en la custodia de los criptoactivos. Hablaremos de la seguridad que confronta la custodia para el mercado de los criptoactivos, señalando las deficiencias y los casos de fraude y fallos a gran escala, que hace resaltar aún más lo interesante del tema.

En el tercer capítulo profundizamos más en el derecho, recalcando los requisitos exigidos de los proveedores de servicios de los criptoactivos divididos en diferentes artículos, y terminaremos con un análisis de MiCA, poniendo a prueba su estructura. La última parte del trabajo está destinada a las conclusiones obtenidas una vez realizado el tema a tratar y sus fuentes bibliográficas.

1. LA REGULACIÓN DE LOS CRIPTOACTIVOS: UNA VISIÓN GENERAL

1.1. Introducción

La aparición de los criptoactivos ha revolucionado el panorama financiero global dando paso a una época, denominada era digital, y a un contexto de alegalidad respecto de muchos aspectos que rodean las operaciones con criptoactivos[1]. La evolución de los criptoactivos y la aparición de ofertas de criptomonedas, como una nueva forma de recaudar dinero utilizando monedas y fichas, ofrecen a las empresas nuevas e innovadoras, especialmente a las pymes, una forma diferente de recaudar capital, pero con claros riesgos que los legisladores deben intentar disminuir o eliminar, en la medida de lo posible. Todo ello se debe especialmente al alto nivel de volatilidad de los criptoactivos, a la capacidad que tiene un ecosistema cripto de eludir la regulación existente, la poca transparencia que rodea las operaciones o la falta de protección de los inversores. Resultando evidente la necesidad de adaptar el marco normativo existente a este fenómeno ya mundial de los criptoactivos, incluso la aprobación de reglas jurídicas específicas en aras de transparencia, trazabilidad de las operaciones, protección de los inversores y, en especial, de los consumidores, libre competencia, estabilidad financiera, integridad de los mercados con evitación de usos indeseados de los capitales (supuestos de blanqueo o financiación del terrorismo), entre muchos otros objetivos también merecedores de protección y que evidentemente requieren reglas jurídicas que permitan una supervisión efectiva de las operaciones con criptoactivos[2].

Éste es el contexto en que se ha sentido la necesidad de aprobarse un reglamento específico para ser aplicado a los criptoactivos, visto que los criptoactivos presentan desafíos regulatorios propios y son muy diferentes a los instrumentos financieros tradicionales, ya regulados. Así, y sin existir una experiencia previa suficiente en criptoactivos, el legislador europeo se ha propuesto "revolucionar" el Derecho con la aprobación del Reglamento

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, disponible online URL: https://bitcoin. org/bitcoin. pdf, 2008, vol. 4, no 2, p. 15. [ultima consulta 09.02.2025]

[2] Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité Europeo de las Regiones; Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador*, Bruselas, 8.3.2018 COM (2018) 109 final, págs. 1-20

MiCA[3] y lo ha hecho dejando su huella característica, a saber, siguiendo, en la medida de lo posible, las mismas líneas de actuación que en la Directiva MIFID II y demás normas reguladoras de los mercados financieros y electrónicos en general, sin perjuicio de innovar ahí donde le ha resultado imprescindible, algunas veces con mayor acierto que otras, según apuntaron los juristas y vamos a desarrollar en el cuerpo de este trabajo, si bien, haciendo referencia a lo que es nuestro objeto de estudio: la custodia de los criptoactivos.

Sobre este último aspecto (aciertos, desaciertos regulatorios y otros problemas derivados de la aplicación del Reglamento MiCA), cabe adelantarse la existencia de una doctrina muy crítica con este reglamento "joven" al que se le tacha de ineficiente. Por ejemplo, según los profesores Zetzke y Nikolakopoulou[4], el Reglamento no consigue acabar hoy con la desconfianza en estos mercados, en especial para los inversores que siguen asumiendo incluso con el Reglamento MiCA serios riesgos. Se reprocha al legislador europeo que el Reglamento MiCA no innova lo suficiente, utiliza una terminología muchas veces confusa, y con significados diferentes en los distintos EE.MM. en que se aplica. Incluso, se reprocha al Reglamento no tomar en consideración las diferencias existentes entre los marcos jurídicos nacionales, aplicables a los contratos que puedan celebrarse sobre criptoactivos en los distintos EE.MM., lo que no solo resulta perjudicial para la transparencia de estos mercados, sino que puede redundar en serios riesgos para los inversores. De alguna forma, la situación se imputa a la "más que evidente" tendencia del legislador europeo de asimilar en demasía los mercados financieros digitales a los tradicionales, a pesar de la peligrosidad que esto entraña en el contexto de unos criptoactivos con características propias y muy diferentes de los productos financieros tradicionales. Con el resultado futuro y previsible de que el Reglamento quede desfasado pronto, vista además la vertiginosa evolución de los criptoactivos[5].

Incluso se ha defendido que este fenómeno mundial de los criptoactivos solo puede ser supervisado de forma efectiva mediante una colaboración internacional que armonice las

---

[3] 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. o 1093/2010 y (UE) n. o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, de aquí en adelante Reglamento MiCA.

[4] Zetzsche, Dirk Andreas and Nikolakopoulou, Areti, "Crypto Custody and Crypto Wallets – An Empirical Assessment" – (March 22, 2024). Available at SSRN: https://ssrn.com/abstract=4769396 or http://dx.doi.org/10.2139/ssrn.4769396. [ultima consulta 09.02.2025]

[5] Zetzsche, Dirk, Andreas and Sinnig, Julia (2024), "The EU Approach to Regulating Digital Currencies" (January 26, 2024). *Law and Contemporary Problems*, Vol. 87, No. 2, Available at SSRN: https://ssrn.com/abstract=4707830 or http://dx.doi.org/10.2139/ssrn.4707830.

regulaciones para evitarse lagunas que puedan ser aprovechadas por individuos mal intencionados[6]. Cabe citarse, a efectos de señalarse la importancia del mercado de los criptoactivos para el sistema financiero mundial y la importancia de una regulación fruto de colaboración internacional, que los datos concretos estudiados señalan que el mercado de los criptoactivos ha llegado a captar en capital aproximadamente 500.000 millones de dólares americanos en 2022, y que se espera que alcance, hasta 2028, los 1601 billones de dólares. Unas cifras cuantiosas que justificarían una colaboración entre los legisladores para evitar un nuevo annus horribilis para el ecosistema cripto, como fue el 2022, con la desaparición -sin rastro- de miles de millones de dólares americanos en valor de mercado[7]. De aquí la necesidad de medidas legales urgentes y eficientes, en un contexto global y coordinado. Idea que comparten muchos autores internacionales que han estudiado los problemas de estos mercados[8].

Vista la complejidad, los riesgos y el auge de los mercados de criptoactivos, no pueden sorprender los esfuerzos pioneros de la Comisión Europea para regular los criptoactivos en Europa, con el Reglamento MiCA, en búsqueda de un crecimiento sano de este nuevo ecosistema financiero que -indudablemente- ha aparecido para marcar la evolución futura de los mercados financieros[9]. A continuación, en esta primera parte del trabajo se intentará motivar la necesidad del citado reglamento para completar las lagunas existentes en el marco jurídico vigente en el momento de su entrada en vigor y aplicable a la custodia de los instrumentos financieros tradicionales. Con especial mención a la Directiva MIFID II[10], que se utiliza como elemento de comparación.

1.2. La necesidad del Reglamento MiCA para regularse los criptoactivos

---

[6] Blandin, A., Cloots, a. s., Hussain, H., Rauchs, M., Saleuddin, R., Eliott, b., ... & Zhang, B. Z. (2019). *Global Cryptoasset Regulatory Landscape Study*. Cambridge Centre for Alternative Finance, Faculty of Law, Research Paper,nº23.

[7]Fantato, Damian (2022) "Crypto and Digital Assets Summit", *Financial Times Events* (Nov. 28, 2022), págs… disponible en https://www.ftadviser.com/events-awards/2022/11/28/crypto-digital-assets-summit.

[8] Burroughes, Tom(2022), "FTX Collapse May Prompt Big Regulatory Crackdown – Lawyer*", Wealth Briefing Asia* (Nov. 18, 2022), https://www.wealthbriefingasia.com/article.php?id=196248.

[9] Sobre el desarrollo de los objetivos que condujeron a esta iniciativa legislativa, 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, COM/2020/593 final, disponible online en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020PC0593.

[10] 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, DOUE de 12.06.2014, página L173/349 y ss.

1.2.1. Algunas cuestiones previas

Como todos sabemos, los criptoactivos son representaciones digitales de un valor o de un derecho, que solo existen cuando se genera digitalmente el criptoactivo a favor de su titular, al que se le facilita una clave pública y otra privada que dan acceso al criptoactivo y otorgan al titular el derecho a controlar y utilizar el criptoactivo. En términos más sencillos, la clase pública puede compararse con el número de una cuenta bancaria, mientras que la clave privada equivale al código PIN o a la firma de un documento bancario necesario para realizarse una transferencia de fondos[11]. Es decir, en el contexto tradicional, los bancos son los custodios de los fondos, pero en un ecosistema cripto no existen bancos, porque nos vamos a encontrar con una encriptación mediante clave pública que permite a una persona, o a un proveedor de servicios que actúe en beneficio de su cliente, poder acceder a los criptoactivos de una cadena de bloques (blockchain) y a mantener el control exclusivo de estos instrumentos financieros digitales, utilizando claves, direcciones o monederos electrónicos. A su vez, las claves privadas tienen la función de permitir al titular realizar operaciones y transacciones financieras digitales con los criptoactivos que posee. Dicho de otro modo, mientras que cualquier persona puede transferir criptoactivos a la dirección de un monedero en una cadena de bloques utilizando la clave pública correspondiente, solo la persona que controla la clave privada encriptada tiene el acceso y el control efectivo de los criptoactivos. De tal modo que la pérdida de la clave privada equivale -en términos informáticos- a la pérdida de los criptoactivos vinculados a una determinada clave pública. Evitar situaciones así fue uno de los objetivos del legislador europeo, tal y como puede entreverse de lo dispuesto en el art. 3.1.17 del Reglamento MiCA al hacer recaer en los proveedores de servicios de criptoactivos (custodios) la obligación novedosa de custodia y administración de criptoactivos por cuenta de clientes (custodia definida 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[12]. no claves públicas, sino privadas. Un reto complejo e importante para el legislador, por todas las implicaciones que

[11] De Filippi and Wright, Aaron, *Blockchain and the Law: the Rule of Code* Harvard University Press , Harvard,2018.

Johnson, Leighton, *Security Controls Evaluation, Testing, and Assessment Handbook*, 2ª ed., Academic Press, Oxford, 2020, pp. 524-526.

[12] Zetzsche, dirk Andreas and Nikolakopoulou, Areti (2024), "Crypto Custody and Crypto Wallets – An Empirical Assessment" – (March 22, 2024), disponible online en https://ssrn.com/abstract=47396 or http://dx.doi.org/10.2139/ssrn.4769396.[ultima consulta 09.02.2025]

supone darse el acceso o la posibilidad de recuperar las claves privadas a otra persona (custodio) que no sea el titular de los criptoactivos. Reto al que se pretende responder con la aplicación de las disposiciones de este Reglamento, cuyos eventuales efectos prácticos debatiremos más adelante.

Nos acercamos de esta forma al tema concreto del trabajo -la custodia de los criptoactivos en el citado Reglamento- que supone, respecto del texto de la Directiva ya existente MIFID II, un paso legislativo incuestionablemente innovador en algunos puntos, por varias razones que se expondrán más adelante en este trabajo. Pero, por razones metodológicas y para facilitarse la comprensión de las disposiciones del Reglamento, antes debemos realizar algunas breves referencias, al menos, al texto de la citada directiva, la principal fuente de inspiración del legislador a la hora de redactar las disposiciones aplicables a la custodia de los criptoactivos en el Reglamento MiCA, porque resultaría imposible un análisis separado del Reglamento MiCA, vista la estrecha relación que existente entre estas normas, por haber intentado el legislador europeo aprovechar para la redacción del Reglamento la experiencia previamente adquirida en los mercados financieros tradicionales.

1.2.2. Respecto del ámbito de aplicación de la MiFID II y MiCA

El principal problema relacionado con el ámbito de aplicación de estas dos normas (Directiva MiFID II y el Reglamento MiCA) gira en torno a las diversas interpretaciones jurídicas ofrecidas en Europa al concepto de "instrumento financiero" y a la cuestión de si un criptoactivo debería o no ser considerado "instrumento financiero". Si un criptoactivo fuera considerado instrumento financiero, en principio, debería quedar sujeto a la aplicación de MiFID II, mientras que, en caso contrario, entraría dentro del ámbito de aplicación del Reglamento. Un problema que se pretende resolver hoy, después de la entrada en vigor del Reglamento, a iniciativa de la Autoridad Europea de Valores y Mercados (ESMA)[13] en busca de un criterio común aplicable por todos los EE.MM. a la hora de valorarse en qué condiciones un criptoactivo debería o no ser considerado instrumento financiero, con lo que pretende proporcionarse en futuro mayor seguridad jurídica y claridad respecto de la interpretación de los artículos que delimitan los ámbitos de aplicación de las citadas normas

[13] Documento de consulta publicado el día 29 de enero de 2024 en https://www.esma.europa.eu/sites/default/files/2024-07/ESA_2024_12_Consultation_Paper_Art_97_MiCA_Guidelines.pdf

europeas. Unas normas europeas que, dicho sea de paso, dejando mucho margen de interpretación a los legisladores nacionales.

Por ejemplo, la Directiva MiFID II proporciona una definición de los instrumentos financieros que se limita al listado ejemplificativo recogido en su anexo I, sección C, por remisión de lo dispuesto en su art. 4.1. Una técnica legislativa de delimitación "enumerativa" de su ámbito objetivo de aplicación que es muy diferente a la empleada en el Reglamento MiCA respecto de la definición de un criptoactivo.

Por su parte, el Reglamento, en su art. 3, define un criptoactivo en términos muy amplios como "una representación digital de un valor o de un derecho que puede transferirse y almacenarse electronicamente, mediante la tecnología de registro distribuido o una tecnología similar". Es decir, el Reglamento procede a la inversa, dicho lo cual, puesto que un criptoactivo no siempre cumpliría todos los requisitos necesarios para considerarse incluido en alguno de los tipos de productos financieros citados en el Anexo de la Directiva MiFID II, se garantizaría de todos modos su regulación, con evitación de un contexto de alegalidad para algún supuesto en concreto. Por lo que se ha defendido -en principio- la más que evidente necesidad de este Reglamento para regular los criptoactivos en general[14]. Sin embargo, el Reglamento, junto a esta definición muy abstracta, recoge algunas excepciones aplicables a su ámbito de aplicación, por lo que para entenderse su verdadero sentido y alcance debe recurrirse a lo dispuesto en su art. 2.4 del siguiente tenor literal:

El presente Reglamento NO se aplicará a los criptoactivos que se consideren:

- a) instrumentos financieros;

- b) depósitos, incluidos los depósitos estructurados;

- c) fondos, excepto si se consideran fichas de dinero electrónico;

- d) posiciones de titulización en el contexto de una titulización, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/2402;

- e) productos de seguro de vida o distintos del seguro de vida pertenecientes a los ramos de seguros enumerados en los anexos I y II de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo (27) o los contratos de reaseguro y de retrocesión a que se refiere dicha Directiva;

[14] Legal Nodes (2023), "The EU Markets in Crypto-Assets (MiCA) Regulation Explained", [en línea], *Legal Nodes*, https://legalnodes.com/article/mica-regulation-explained [ultima consulta 09.02.2025]

- f) productos de pensiones que, con arreglo al Derecho nacional, tengan reconocida como finalidad primaria la de proveer al inversor de unos ingresos en la jubilación y que les den derecho a determinadas prestaciones;

- g) planes de pensiones de empleo reconocidos oficialmente incluidos en el ámbito de aplicación de la Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo o de la Directiva 2009/138/CE;

- h) productos de pensión individuales en relación con los cuales el Derecho nacional exija una contribuciónn financiera del empleador y en los que ni el empleador ni el empleado tengan posibilidad alguna de elegir el producto de pensión ni a su proveedor;

- i) un producto paneuropeo de pensiones individuales, tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2019/1238 del Parlamento Europeo y del Consejo (29);

- j) sistemas de seguridad social a los que les sean de aplicación los Reglamentos (CE) nº. 883/2004 (30) y (CE) nº. 987/2009.

Todas estas excepciones tienen su sentido en la medida en que se trata de supuestos ya regulados en normas especiales antes de la entrada en vigor del Reglamento, con lo que podemos observar que el Reglamento MiCA pretende abarcar aquellos productos y servicios financieros todavía no regulados (interpretación dada al art. 2.4), excluyendo también los criptoactivos no fungibles -NFTs (art. 2.3). Y la situación no ha sido exenta de polémica, sino todo lo contrario, ya que ha conducido a una interpretación divergente en distintos EE.MM., debido a legislaciones nacionales que definen de forma diversa conceptos claves como "instrumento financiero" o "valor mobiliario", en un contexto en que el texto del Reglamento, por su ambigüedad, no facilita una interpretación uniforme de los conceptos. Se ha criticado así, por ambigua, la forma de redacción del art. 2.4, al no proporcionar un listado exhaustivo de los criptoactivos excluidos de su ámbito de aplicación. En términos intuitivos, podríamos señalar que un instrumento financiero es, al fin y al cabo, un contrato monetario, lo que de por sí no excluye que un criptoactivo se considere instrumento financiero. Es decir, debía haberse delimitado claramente los requisitos que ha de reunir un instrumento financiero para entrar claramente dentro del ámbito de aplicación de alguna de estas dos normas, con excepción de la otra. Un problema interpretativo cuya solución depende del resultado que tenga la consulta lanzada por la ESMA[15] que, en el Anexo C del

[15] Primero, en opinión de la ESMA, los términos valor y derecho deben interpretarse en sentido muy amplio, según considerando 2º del Reglamento.

El valor de un criptoactivo puede determinarse en función del valor de una moneda de curso oficial o de otros valores como el oro o, más nuevo, utilizándose el valor de la red que utiliza como medio de intercambio el token en cuestión (tendrán en este contexto importancia primordial la velocidad de circulación del criptoactivo y las expectativas de los agentes económicos sobre el éxito de la plataforma de servicios y/o productos que emite los activos). Para más detalles respecto de estas teorías cuantitativas del dinero y las

documento, incluye además un esquema que facilita en cierto modo la interpretación del Reglamento, si bien se aconseja la necesidad de realizarse, caso por caso, un análisis individualizado de cada tipo de criptoactivo para llegarse a un resultado correcto. Pues, el valor de un criptoactivo y los derechos que pueda conceder un criptoactivo a su titular no son lo mismo, con lo que el análisis puede conducir a un resultado diferente (es decir, a la aplicación o no del Reglamento MiCA al negocio jurídico en cuestión).

Para sintetizar, y a pesar de los problemas expuestos, podríamos señalar que el título II del Reglamento cubre con carácter general los criptoactivos distintos de una ficha referenciada a activos o fichas de dinero electrónico, mientras que el título III cubre en específico las fichas referenciadas a activos (ARTs) -es decir, tokens cuyo valor se calcula tomando como referencia otro valor, otro derecho, o una combinación de valores y derechos- y el título IV cubre las fichas de dinero electrónico (EMTs) -tokens cuyo valor se referencia atendiendo al valor de una moneda oficial-. Todo lo que debe interpretarse en el sentido del considerando 22 del Reglamento. Es decir, cuando los criptoactivos no tengan un emisor identificable no deberían entrar en el ámbito de aplicación de los títulos II, III o IV del presente Reglamento, aunque, de todos modos, -en opinión de algunos autores- los proveedores de servicios de criptoactivos que presten servicios en relación con tales criptoactivos deban, aun así, entrar dentro del ámbito de aplicaciónn del presente Reglamento para someterse a las obligaciones que derivan con carácter general del Reglamento MiCA para los proveedores de servicios de criptoactivos. Lo que también se aplicaría respecto de la custodia de los criptoactivos, según el tenor literal del considerando 22. Considerando que apunta, como uno de los objetivos del Reglamento MiCA, someter a todos los proveedores de servicios de criptoactivos, independientemente de las particularidades señaladas, a las mismas exigencias. Una medida necesaria y proactiva ante

---

derivadas de la denominada economía de las redes, vid. Prosper Lamothe Fernández, Prosper Lamothe López, ¿Cómo valorar los denominados criptoactivos?, pp. 1-10, disponible online en https://www.funcas.es/wp-content/uploads/2020/08/CIE277art09.pdf.

Asimismo, el criptoactivo como derecho puede implicar el derecho del titular a recibir un determinado bien, servicio o importe, el derecho de tener acceso a utilizar un bien o servicio, incluso el derecho de reproducción de una obra. Señalarse también que un criptoactivo sin valor intrínseco, cuyo valor se determina libremente por el vendedor, comprador o por los participantes en el mercado debe considerarse, en todo caso, activo con valor digital (ej. Bitcoin), según se recoge en el documento de consulta de la ESMA.

Segundo, y siguiendo la misma opinión de la ESMA, debería cumplirse -en los términos fijados por los EE.MM. - el requisito de tratarse de valores o derechos transferidos y adquiridos digitalmente, utilizándose tecnología DLT (distributed ledger technology) o similar.

Dos criterios que, una vez cumplidos, harían aplicable el Reglamento a los criptoactivos, siempre y cuando no se trate de la emisión de un criptoactivo en el sentido del art. 2.2 del Reglamento, siempre que el criptoactivo sea único y no fungible con otros criptoactivos y no excluido expresamente del ámbito de aplicación del Reglamento por el art. 2.4.

las nuevas realidades del mercado financiero impulsadas por la tecnología blockchain y los criptoactivos[16], similar a la adoptada -en su día- respecto de las obligaciones de custodia impuestas a las entidades que prestan servicios de inversión o a las entidades de crédito tradicionales en la Directiva MiFID II. Sin poderse romper el análisis de las disposiciones del Reglamento MiCA de toda la demás legislación financiera europea, si se desea realmente entenderse su alcance, por ser este marco jurídico la principal fuente de inspiración del legislador europeo[17].

Para facilitarse la transición hacia el nuevo marco regulador, el Reglamento permite además a los proveedores de servicios de criptoactivos operar de igual forma hasta el 1 de julio de 2026, a hasta la fecha en que se les conceda o deniegue una nueva autorizaciónn conforme al Reglamento. Un enfoque gradual que queda, de todos modos, a apreciación de los EE.MM. que podrán matizarlo en atención a las diferencias existentes entre las disposiciones del Reglamento y sus Derechos internos. Lo que resulta fundamental para evitarse la fragmentación regulatoria y promoverse un mercado único más integrado y eficiente y que se aplica también a las disposiciones relativas a la custodia de los criptoactivos que recoge el Reglamento[18].

1.2.3. La necesidad de reglas especiales de custodia para los criptoactivos

Brevemente, y por su importancia como antecedente, debe señalarse que la Directiva MiFID II pretendía mejorar las disposiciones recogidas en normas anteriores. Unas normas que además modifica en ciertos aspectos, como es el caso -por ejemplo y respecto del deber de custodia de los instrumentos financieros- de la Directiva 2011/61/UE.

La citada Directiva de 2011 establece claras diferencias entre las funciones de custodia y gestión de los activos, y entre los activos de los inversores y de los del gestor. De modo que, por ejemplo, en lo que respecta la custodia de los activos, respalda el

---

[16] Schär, F. (2021). "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets", *Federal Reserve Bank of St. Louis Review*, Vol. 103, No. 2, pp. 153-174.

[17] Zetzsche, Dirk Andreas, Sinnig, Julia, (2024)"The EU Approach to Regulating Digital Currencies" (January 26, 2024). *Law and Contemporary Problems*, Vol. 87, No. 2. Available at SSRN: https://ssrn.com/abstract=4707830.

[18]. Madrid Parra, Agustín (coord.). et al, *Guía de criptoactivos MiCA*, Aranzadi, Pamplona, 2021

nombramiento de depositarios distintos de un GFIA (gestores de fondos de inversión alternativos) para ejercer las funciones de depósito en relación con los FIA (fondos de inversión alternativos). Todo ello orientado a minimizarse los conflictos de intereses que puedan surgir. También deben destacarse los esfuerzos del legislador, dada la importancia de la función de custodia, de garantizar en todos los casos la implicación en las operaciones financieras de depositarios entidades de crédito, empresas de inversión u otra entidad permitida en virtud de la Directiva 2009/65/CE. Unos depositarios a los que se le encomienda la custodia de los activos del FIA, incluida la de los instrumentos financieros que puedan consignarse en una cuenta de instrumentos financieros abierta en los libros del depositario y todos los demás instrumentos financieros que puedan entregarse físicamente al depositario, con verificación de la propiedad de todos los demás activos FIA o del GFIA cuando se actúe por cuenta de éste. La custodia de los activos se aborda también en términos de poder delegarse o subdelegarse en terceros esta función, bajo la condición de estar objetivamente justificada una delegación/subdelegación y atenerse a requisitos estrictos sobre la idoneidad del tercero al que se confíe tal función, y sobre la competencia, el esmero y la diligencia que el depositario debe demostrar a la hora de seleccionar, nombrar y supervisar al tercero en cuestión. Con imposición a este tercero de la obligación de llevar una cuenta separada común para múltiples FIA ("cuenta ómnibus")[19]. Asimismo, en supuestos de liquidaciones firmes de sistemas de pagos y de valores, se confía la custodia de los activos al operador de un sistema de liquidaciónn de valores designado por los sistemas de liquidación de valores o la prestación de servicios similares por parte de sistemas de liquidación de valores de terceros países no se debe considerar delegación de las funciones de custodia.

Finalmente, señalarse que a los depositarios se les sanciona con ser responsables de las pérdidas sufridas por el GFIA, el FIA y los inversores, con clara distinción entre la pérdida de instrumentos financieros custodiados y cualquier otro tipo de perjuicio -en este último caso- si el depositario hubiera obrado con dolo o negligencia. Asimismo, debe destacarse la regla que fija la Directiva, de conformidad con la cual "cuando el depositario custodie activos y se pierdan, el depositario debe ser responsable, a menos que pueda probar que la pérdida se ha producido como resultado de un acontecimiento externo que escape a un control razonable, cuyas consecuencias hubieran sido inevitables pese a todos los esfuerzos razonables por evitarlas. En este sentido, un depositario no debe poder invocar determinadas situaciones internas, como un acto fraudulento por parte de un empleado, para eximirse de

[19] Sobre estos aspectos, citarse en especial los considerandos 39 y 40 de la Directiva.

su responsabilidad. En caso de delegación o subdelegación, también resultara responsable el depositario si no media una cesión contractual expresa de dicha responsabilidad a cargo del tercero, según se explica en el considerando 45 de la Directiva. Otras excepciones se recogen respecto de operaciones realizadas con un tercer país, en los términos señalados, a modo de ejemplo, en el considerando 49[20].

Por su parte, el art. 21.8 de la citada Directiva de 2011 se encarga específicamente de fijar los concretos términos en que debe llevarse a cabo la custodia de los activos:

Para los activos FIA o GFIA cuando se actúe por cuenta del FIA, los mismos se confiarán al depositario para su custodia del modo siguiente:

a) instrumentos financieros que se pueden tener en custodia:

> i) el depositario tendráá en custodia todos los instrumentos financieros que puedan consignarse en una cuenta de instrumentos financieros abierta en los libros del depositario y todos los instrumentos financieros que puedan entregarse fisicamente al depositario,
>
> ii) a tal fin, el depositario garantizará que todos los instrumentos financieros que puedan consignarse en una cuenta de instrumentos financieros abierta en los libros del depositario se consignen en los libros del depositario en cuentas separadas, de conformidad con los principios establecidos en el artículo 16 de la Directiva 2006/73/CE, abiertas a nombre del FIA o, en su caso, del GFIA cuando actúe por cuenta del FIA, de modo que se puedan identificar claramente como pertenecientes al FIA, de conformidad con la legislación aplicable en todo momento;

b) para otros activos solo se establece la obligación de mantenerse un registro actualizado, en las condiciones que fija el citado artículo.

Sin necesidad de realizarse un análisis exhaustivo de este marco regulatorio aplicable a la custodia de activos financieros tradicionales según la citada Directiva de 2011, debe

[20] "Cuando la legislación de un tercer país exija que ciertos instrumentos financieros sean mantenidos en custodia por una entidad local y no haya entidades locales que satisfagan los requisitos de delegación de la custodia, el depositario debe poder quedar exento de su responsabilidad siempre que: el reglamento o los estatutos del FIA en cuestión autoricen expresamente dicha exención de responsabilidad; los inversores hayan sido debidamente informados de dicha exención de responsabilidad y de las circunstancias que la justifican antes de la inversión; el FIA o el GFIA cuando actúe por cuenta del FIA hayan pedido al depositario que delegue la custodia de dichos instrumentos financieros en una entidad local; haya un contrato escrito entre el depositario y el FIA o, en su caso, el GFIA cuando actúe por cuenta del FIA por el que se permita expresamente dicha exención de responsabilidad; y exista un contrato escrito entre el depositario y el tercero por el que se transfiere expresamente la responsabilidad del depositario a dicho tercero y se autoriza al FIA o, en su caso, al GFIA cuando actúe por cuenta del FIA a presentar una reclamación contra el tercero en relación con la pérdida de instrumentos financieros o al depositario a presentar tal reclamación en su nombre".

señalarse que la Directiva MiFID II lo mantiene, para ampliarlo a los servicios auxiliares citados en su Sección B, sin que en ningún caso pueda autorizarse únicamente la prestación de servicios auxiliares, y simplificando los trámites administrativos para los GFIA autorizados por las autoridades competentes de su Estado miembro de origen a proporcionar estos servicios, en el sentido de no tener que verse sujetos a una autorización suplementaria en los Estados miembros de acogida, ni a ninguna otra medida de efecto equivalente (el así llamado "pasaporte europeo").

De lo expuesto respecto a este marco regulatorio podemos fácilmente observar que se trata de la regulación de un sistema financiero centralizado, es decir, en que siempre existirá una entidad/autoridad que controle los activos financieros y el flujo de dinero y donde las entidades de crédito, las entidades de inversión y otras entidades autorizadas legalmente van a jugar siempre un papel primordial como intermediarios de las operaciones. Sin embargo, esta situación ni se da siempre, ni con la misma intensidad en el caso de los criptoactivos. Cuando nos referimos a los criptoactivos, nos referimos a un ecosistema de aplicaciones descentralizadas, conocido como DeFi, que no necesita de una autoridad central, ni de intermediarios para la realización de las operaciones. Si bien, este ecosistema admite en algunas situaciones y hasta un determinado nivel la concentración, lo que hace posible que pueda identificarse en ocasiones algún intermediario implicado, por ejemplo, en la creación o lanzamiento de un determinado activo, cobrando tarifas o realizando alguna labor administrativa vinculada a los criptoactivos y/o a las plataformas en las que se opera. Pues bien, el legislador europeo ha pretendido regular -al menos- estas situaciones en las que a alguna persona física o jurídica pueda imponerle deberes de custodia, por no resultar ajena a las operaciones financieras ya que lanza o provee servicios de criptoactivos. Es decir, el Reglamento MiCA solo se aplica en caso de poderse identificar alguna persona física o jurídica que cumpla estas condiciones. Con lo que operaciones con criptoactivos basadas en modelos totalmente descentralizados como los denominados "smart contracts" no entrarían dentro del ámbito de aplicación del Reglamento[21]. Podríamos decir que la regulación de la custodia de los criptoactivos no ha llegado todavía a un nivel capaz de abarcar los "smart contracts", porque estamos frente a un reglamento que -como vamos a poder observar más adelante- pretende imponer deberes similares a las recogidas en la Directiva MiFID y hasta aquí citadas, a personas físicas o jurídicas denominadas "custodios" de criptoactivos.

[21] Maia, Guilherme; Vieira dos Santos, João, "MiCA and DeFi (*Proposal for a Regulation on Market in Crypto-Assets' and Decentralised Finance)"*, *Revista Electrónica de Direito.* RED, vol. 28, nº.2, 2022, pp.57-82.

En este contexto, algunos autores consideran viable la aplicación futura del reglamento "a alguna actividad, a algunos riesgos o en algunas condiciones", y señalan el importante riesgo de convertirse pronto en una legislación obsoleta, prácticamente ineficiente o aplicable solo de forma residual en los EE.MM., porque el crecimiento del DeFi y la innovación tecnológica que marca la evolución de los criptoactivos generan un ambiente muy problemático para el Derecho. Un Derecho que, como la experiencia financiera y jurídica han enseñado, se ha adaptado de forma eficaz a los cambios solo después de producirse éstos en los mercados, sin presagiarse una efectividad remarcable en la práctica para las reglas que introduce el Reglamento MiCA respecto de la custodia de los criptoactivos[22].

Ahora bien, así como ha enfatizado la Autoridad Bancaria Europea, estos retos regulatorios afrontados por el legislador europeo son consecuencia de una clara "expectativa idealista" de descentralización de los mercados financieros[23], percibida como la "democratización" del tradicional sistema financiero centralizado, lo que entraña hoy el claro riesgo, perfectamente definido en el continente americano con el sintagma "el ganador se lleva todo", especialmente cuando las operaciones se concentran en determinadas plataformas que adolecen de transparencia operativa, lo que ha propiciado abusos, casos de fraudes y fallos de todo tipo y a gran escala[24].

En conclusión, y sin perjuicio del estudio que sigue respecto del modelo de custodia de los criptoactivos en el Reglamento MiCA, que fija obligaciones y responsabilidades concretas para los custodios de criptoactivos, no debe olvidarse que se trata de un primer intento legislativo, pionero en el mundo, muy necesario para los mercados de los criptoactivos, pero a prueba del paso del tiempo y de una innovación tecnológica vertiginosa que lo va a poner a importantes pruebas en la práctica, con la expectativa de un pronto

---

[22] D. Zetzsche, F. Annunziata, D. Arner, and R. Buckley, "The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy" (2021), en 16(2) Capital Markets Law Journal, E. Noble, "Crypto-Assets – Overcoming Impediments to Scaling" (2020); Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748343,[ultimately consulta 9/02/2025]; J. McCarthy, J.(2021), 'Evaluating the EU's Digital Finance Strategy: Ambitious Glimpses of Future Regulation?', en 36(9) Journal of International Banking Law and Regulation, pág. 379; G. Ferrarini and P. Giudici, "Digital Offerings and Mandatory Disclosure: A Market-Based Critique of MiCA" (European Corporate Governance Institute – Law Working Paper No. 605/2021); disponible online en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3914768 [ultimately consulta [9/02/2025].

[23] EBA, Report on the Use of Digital Platforms in the EU Banking and Payments Sector (EBA/REP/2021/26 (September 2021).

[24] R. Browne, "Criminals have made off with over $10 billion in 'DeFi' scams and thefts this year" Available at : https://www.cnbc.com/2021/11/19/over-10-billion-lost-to-defi-scams-and-thefts-in-2021.html [ultimately consulta 9/02/2025].

fracaso, según resulta de la reciente literatura jurídica citada hasta aquí. Un intento legislativo del que seguramente se va a aprender mucho.

2. LOS CUSTODIOS DE LOS CRIPTOACTIVOS

2.1. Introducción

En Europa durante el siglo XVI y XVII, surgió la figura de los orfebres, quienes gozaban de una gran reputación. Las personas confiaban en ellos y guardaban sus riquezas en sus bodegas, ellos a cambio entregaban una nota o certificado donde establecían cuánto dinero tenían depositado. Eventualmente las personas empezaron a intercambiar estos certificados convirtiéndose en una forma de billetes tal y como lo conocemos.
Los orfebres pudieron observar que las personas dejaban de retirar su dinero y se quedaba de manera permanente en las bodegas, y se dieron cuenta que podían utilizar parte del oro siempre y cuando no todos lo quisieran retirar a la vez, y de esta manera se formó una nueva versión de la banca, algo muy similar al funcionamiento del sistema bancario que conocemos hasta la fecha.[25]

Con la llegada de la Revolución Industrial y el crecimiento de los mercados financieros, la custodia de activos experimentó cambios significativos. Los bancos y otras entidades financieras comenzaron a ofrecer servicios de custodia más avanzados, que incluían la protección de títulos como acciones y bonos. En el siglo XIX, la custodia de valores se formalizó con la introducción de cámaras de compensación y sistemas centralizados de depósito.

El siglo XX marcó una época de globalización financiera sin precedentes. La custodia de activos se volvió más compleja debido al incremento del comercio internacional y a la diversificación de instrumentos financieros. Los depositarios centrales (CSD) y los bancos custodios desempeñaron un papel fundamental en facilitar el comercio transfronterizo y gestionar los riesgos asociados con la custodia. Con el advenimiento digital a finales del siglo XX e inicios del XXI, la custodia de activos vivió una transformación radical. La tecnología posibilitó el desarrollo de sistemas electrónicos que ofrecían mayor eficiencia y seguridad en cuanto a custodia. El surgimiento del Internet y las tecnologías informáticas dio paso a

[25] Inverbots Español. "*La Historia del dinero- El Trueque, Acuñación, Banca y Criptomonedas"*. 21 de Noviembre 2020. https://www.youtube.com/watch?v=-bh3Tt_ZvXQ [ultima consulta 9/02/2025]

nuevos tipos de activos digitales, culminando en la aparición posteriormente conocida como criptoactividad.[26]

En los últimos años, la tecnología blockchain y las criptomonedas han tenido un impacto significativo en el ámbito financiero a nivel mundial. Estos activos digitales no solo han generado nuevas oportunidades de inversión y financiamiento, sino que también han planteado desafíos regulatorios sin precedentes.

2.2. La relevancia de los custodios de criptoactivos

Los custodios desempeñan un papel clave en los mercados financieros y de criptoactivos, asegurando la protección y administración segura de los activos de los inversores. En el marco regulatorio europeo, normativas como MiFID y MiCA establecen requisitos específicos para los custodios tradicionales y los proveedores de servicios de criptoactivos, garantizando transparencia, seguridad y cumplimiento normativo.

Mientras que MiFID regula los custodios en el ámbito de los valores financieros, asegurando la protección de los inversores mediante controles estrictos, MiCA introduce por primera vez una regulación específica para la custodia de criptoactivos, abordando riesgos como la pérdida de claves privadas y la insolvencia de proveedores. La evolución de estas normativas refleja la creciente importancia de los custodios en la estabilidad y confianza de los mercados financieros, tanto tradicionales como digitales.

Para determinar el papel fundamental de los custodios de los criptoactivos, hay que desglosar las seis deficiencias que contribuyeron a que los titulares de los tokens perdieran la confianza de los criptoactivos, debido a que la forma de custodia colectiva ha sido hasta ahora "caliente"[27], lo que significa que el proveedor de la cartera almacena todas las claves privadas de sus clientes juntas en carteras que están permanentemente en línea y vinculadas

---

[26] Saifedean.A. "El patrón Bitcoin", Universidad de Deusto, Bilbao, 2022. Cap.1 "*Dinero*", pp. 23-33.

[27] Los monederos en línea están conectados a internet y se utilizan para acceder rápidamente a las criptomonedas y realizar transacciones con frecuencia. Hay varias formas de monederos en línea, que incluyen aplicaciones móviles, programas de escritorio y servicios web. Algunos ejemplos populares de monederos en línea son: Coinbase Wallet, MetaMask y MyEtherWallet.
Las ventajas de los monederos en línea incluyen la comodidad y la facilidad de acceso. Permiten a los usuarios enviar y recibir criptomonedas rápida y eficientemente, lo que los convierte en una opción ideal para el uso diario y las transacciones frecuentes. Sin embargo, esta constante conexión a internet también los hace más vulnerables a ataques cibernéticos. Los hackers podrían aprovechar vulnerabilidades en el software o utilizar técnicas como el phishing para acceder a los fondos de los usuarios.

al libro mayor distribuido[28]. Este tipo de "carteras ómnibus" son más vulnerables a ataques de internet y brechas de seguridad como adelantamos en el Capítulo 1.[29]

Los custodios de criptoactivos no pudieron evitar la pérdida de claves privadas administradas por ellos en relación con los activos de sus clientes, aplicaron políticas insuficientes para abordar riesgos cibernéticos, robos y fraudes tanto internos como externos, mezclaron el negocio de custodia con actividades de riesgo de intercambios de criptoactivos, corredores, inversiones y préstamos en el mismo balance y también mezclaron numerosos activos de clientes con sus propios activos que no supieron distinguir ni los activos de sus clientes ni los suyos propios como tales[30]. Este fue, por ejemplo, el caso de

---

[28] El libro mayor en MiCA es el sistema de contabilidad digital que registra y verifica transacciones de criptoactivos de manera descentralizada. Puede ser una blockchain pública o privada, dependiendo de su diseño y gobernanza. MiCA no regula directamente la tecnología del libro mayor, pero establece requisitos para los proveedores de servicios que operan con estos registros, garantizando seguridad, integridad y transparencia en la custodia y gestión de criptoactivos.

[29] Entre otros, Gareth Jenkinson, "CoinEx hack: Compromised private keys led to $70M theft" *Cointelegraph*, 2023)https://cointelegraph.com/news/coinex-compromised-private-keys-behind-70-million-hack. [ultimately 9/02/2025]; Siddhartha Shukla, "Crypto Exchange HTX Hit by $258 Million Outflow After Hack",*Bloomberg*,2023 https://www.bloomberg.com/news/articles/2023-12-10.

[30] El mes de mayo de 2022 resultó ser un período tumultuoso para el mercado de criptomonedas, con una serie de eventos significativos que pusieron de manifiesto los riesgos y desafíos asociados con la custodia y gestión de activos digitales.
Terra Luna, una criptomoneda integrada en el ecosistema de Terra, experimentó un colapso devastador en mayo de 2022. Inicialmente concebida como una stablecoin (moneda digital) algorítmica vinculada al valor del dólar estadounidense a través de un mecanismo que implicaba arbitraje y quema de tokens entre Terra (LUNA) y TerraUSD (UST), la situación dio un giro inesperado ese mes cuando la paridad entre UST y el dólar se vio comprometida, desencadenando así una espiral descendente en el valor de LUNA. Las causas subyacentes del colapso incluyen la desvinculación del UST debido a la disminución en su valor por debajo de $1, lo que provocó una ola masiva de ventas que intensificó su depreciación. Además, las deficiencias en el mecanismo algorítmico diseñado para mantener la paridad no pudieron resistir la presión generada por las ventas masivas.
La pérdida generalizada de confianza en el mercado también contribuyó al deterioro del panorama financiero.
La brusca disminución de UST y LUNA generó desconfianza en el proyecto, lo que desencadenó más ventas y una espiral descendente que se alimentaba a sí misma.
Los inversores en LUNA y UST experimentaron pérdidas masivas, con el valor de LUNA cayendo casi a cero.
El colapso de Terra Luna tuvo un efecto negativo en la confianza del mercado de criptomonedas, contribuyendo a una caída generalizada en los precios de los activos criptográficos.
Este evento llamó la atención de reguladores globales, quienes resaltaron la necesidad de una supervisión más estricta y marcos regulatorios para las stablecoins.
Otro impacto en el mercado criptomonetario fue Three Arrows Capital (3AC): un fondo de cobertura especializado en criptomonedas se vio obligado a declararse en quiebra en julio de 2022 tras sufrir pérdidas devastadoras. La empresa había asumido posiciones altamente apalancadas en varias criptomonedas, y la disminución de los precios de los activos digitales durante mayo exacerbó sus problemas financieros.
Las razones detrás del colapso fue que (3AC) tenía una exposición significativa a Terra Luna, derivando esta caída de moneda digital uno de los principales factores que contribuyeron a sus pérdidas.
Las estrategias de inversión arriesgadas como el alto apalancamiento y la falta de diversificación en las inversiones aumentaron la exposición del fondo a las fluctuaciones del mercado.
Las decisiones estratégicas y la ausencia de una gestión adecuada de riesgos por parte de los fundadores de 3AC llevaron a un rápido deterioro de su situación financiera.

las carteras "colectivas" calientes (en línea) donde los activos de múltiples clientes, y generalmente los propios activos del custodio, se mezclan. Otra deficiencia fue ejecutar una contabilidad insuficiente, marcación de activos, controles internos y prácticas de continuidad del negocio, de modo que a posteriori las transacciones en nombre de los clientes no se podían distinguir de las realizadas en nombre de la entidad del custodio[31]. Por último, reutilizaron los activos de los clientes para operaciones comerciales propias en su propia cuenta o en la de una entidad relacionada[32], por lo que se cubrieron con los activos de custodia de los clientes.[33]

Las consecuencias se tradujeron en la incapacidad de 3AC para cumplir con sus obligaciones financieras produciendo la liquidación. Y la quiebra de 3AC afectó a otras empresas y plataformas que habían invertido en, o prestado fondos a 3AC, generando un efecto dominó en el mercado criptográfico.

[31] Voyager Digital y Celsius Network, dos destacadas plataformas de préstamos de criptomonedas, enfrentaron graves dificultades financieras en 2022, lo que condujo a situaciones insolvencia y acusaciones relacionadas con una deficiente gestión y fraude.
Voyager Digital experimentó grandes pérdidas debido a su exposición con 3AC, que no pudo reembolsar los préstamos concedidos por Voyager. En julio del año pasado, Voyager suspendió las operaciones de retiro, depósito y comercio para sus clientes debido a problemas relacionados con la liquidez. La empresa optó por la protección del Capítulo 11 de bancarrota con el fin de reorganizar sus deudas y buscar la forma de devolver el dinero a sus clientes.
Celsius Network se vio envuelta en acusaciones por una gestión deficiente y el uso inapropiado de los fondos de los clientes para llevar a cabo inversiones arriesgadas. En junio de 2022, Celsius detuvo todas las retiradas y transferencias de fondos por problemas de liquidez.
Las acciones realizadas por Celsius provocaron investigaciones legales y regulatorias sobre posibles fraudes y violaciones a leyes financieras.

[32] El colapso de FTX, una de las principales plataformas de intercambio de criptomonedas, marcó un momento crítico durante el invierno criptográfico de 2022-2023. Fundada por Sam Bankman-Fried en 2019, FTX rápidamente se destacó en el mercado de criptomonedas. Sin embargo, en noviembre de 2022, la plataforma enfrentó una crisis de liquidez que resultó en su colapso.
La crisis comenzó cuando un informe reveló que gran parte del balance de Alameda Research, una firma comercial afiliada a FTX, consistía en FTT, el token nativo de FTX. Esto generó preocupaciones sobre la estabilidad financiera de FTX y provocó una ola de retiros por parte de los usuarios.
Binance, uno de los principales competidores de FTX, inicialmente acordó adquirir la plataforma para ayudar a mitigar la crisis. Sin embargo, después de revisar los registros financieros de FTX, Binance se retiró del acuerdo citando problemas con la gestión fondos y falta transparencia, llevando a FTX el 11 de Noviembre de 2022 a bancarrota. Posteriormente, Sam Bankman-Fried fue detenido y acusado de varios delitos financieros, incluyendo fraude y lavado de dinero.
El colapso de FTX resultó tener pérdidas importantes para los inversores y usuarios de la plataforma, con miles de millones de dólares en activos congelados. Este suceso aceleró las investigaciones por parte de reguladores en Estados Unidos y otros países, resaltando la necesidad de una mayor supervisión en el ámbito de las criptomonedas. La quiebra de FTX ha sacudido la confianza en el mercado de criptomonedas, ocasionando una caída en los precios de numerosos criptoactivos y generando escepticismo sobre la viabilidad de las plataformas sin una regulación adecuada.

[33] 20 SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao (Comunicado de prensa, 5 de junio de 2023) https://www.sec.gov/news/press-release/2023-101 [Consulta: 9/02/2025]

Las noticias sobre estas deficiencias se tradujeron en un golpe muy duro a los mercados de criptoactivos en un momento en que estaban emergiendo señales de concentración del mercado. Los clientes iniciaron ventas masivas similares a las corridas bancarias comunes en TradFi. Cuando algunos de los nuevos intermediarios de criptoactivos sistémicamente importantes (SICI) estaban fallando, con riesgos para los titulares de tokens, la estabilidad del mercado y la integridad del mercado de dimensiones sistémicas. Estas ventas masivas revelaron interconexiones y efectos de contagio previamente desconocidos en los mercados de TradFi, socavando aún más la estabilidad de los custodios de criptoactivos.[34]

La Directiva 2014/65/UE establece requisitos y detalla las medidas sobre la financiación tradicional (TradFi) equilibrando las consideraciones de coste y de protección del cliente. Un custodio en el primer nivel de la cadena de custodia (es decir, un custodio que establece una relación contractual con el cliente) tiene la obligación legal de proporcionar una cuenta totalmente segregada para cada uno de sus clientes individualmente y de registrar adecuadamente los activos de cada cliente en los libros y registros del custodio. Esta doble obligación garantiza la protección de los activos de cada cliente contra los riesgos de insolvencia.[35]

La normativa TradFi prevé, además, que, si el depositario delega la custodia en un tercero, este tercero está autorizado a gestionar cuentas ómnibus. Esta mezcla en el segundo nivel es una necesidad técnica para evitar la indeseable situación en la que, en una configuración jerárquica de la cadena de custodia, todos los datos del cliente deben remitirse al delegado y conciliarse con él. Incluso entonces, una cuenta ómnibus operada por el tercero deberá excluir los activos propios del custodio delegante, los activos propios del tercero, así como los activos de los demás clientes del tercero. Por esta razón, es importante señalar que una cuenta ómnibus en TradFi es siempre una cuenta colectiva de activos mantenidos únicamente por cuenta de clientes; los activos de los custodios, y de cualquier custodia de terceros, según sea el caso, están excluidos. En segundo lugar, el depositario y cualquier tercero encargado de la custodia están obligados a mantener registros y libros detallados que muestren la segregación, de modo que estén en condiciones de identificar en cualquier

[34] Arner,Zetzsche,Buckley,Kirkwood, "The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-202", Universidad de Hong Kong, 2023. [ultimately consulta 9/02/2025]

[35] Cf. GFIA, art 11(d); OICVM, art 22a (3); Reglamento Delegado (UE) 2018/1618 de la Comisión, art 2(1)(d)

momento y sin demora los activos pertenecientes a cada cliente individual, como se explica más adelante.[36]

Las numerosas quiebras de custodios de criptoactivos que ocurrieron en las cercanías de estos eventos revelaron además que, cuando los titulares de tokens dependían más de sus custodios, los custodios prominentes no podían cumplir con su promesa de salvaguardar los activos de sus clientes.[37] Los procedimientos de insolvencia hicieron transparente que la adecuada segregación de activos, la continuidad del negocio y los enfoques de recuperación, así como otras buenas prácticas de custodia, estaban ausentes en toda la industria. Los clientes quedaron completamente desprotegidos, mientras que las leyes de propiedad e insolvencia de criptoactivos, emergentes pero fragmentarias en la mayoría de las jurisdicciones, hicieron poco para fomentar la protección privada de los propios titulares de tokens.[38]

En general, estos casos plantean la cuestión de si el término "custodio" sería el término adecuado para este tipo de servicio de criptoactivos, ya que, al fin y al cabo, muy poco se mantuvo "en custodia" o se salvaguardó en absoluto.

En la legislación financiera relativa a la custodia de instrumentos financieros, la noción de custodia está más reforzada, pero con debilidades, ya que no existe una definición clara y uniforme de lo que constituye la custodia de activos. En la legislación pertinente suele figurar una lista de todas las obligaciones de custodia que debe asumir un custodio, en función del tipo de custodio y del tipo o tipos de activos custodiados. [39]

---

[36] Sobre la admisibilidad de las cuentas ómnibus de los depositarios de fondos, véase GFIA, art. 21.

[37] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & van Ek, M. (2023), *Remaining regulatory challenges in digital finance and crypto-assets after MiCA, Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies,* European Parliament, Luxembourg (2023): 23-27.

[38] Woxholth, Jannik; Zetzsche, Dirk AndreasM; Buckley, Ross P. y Arner, Douglas W., "Competing Claims to Crypto assets", Uniform Law Review, vol. 28, t. 2, 2023, pp. 226–246.

[39] En cuanto a las obligaciones de custodia del depositario del fondo, véase la 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 (GFIA) [2011], DO L 174/1, art. 21 (8)

El denominador común de las obligaciones de custodia en la legislación financiera es el siguiente: para los activos financieros que pueden ser custodiados, la noción central y *conditio sine qua non* de la custodia es el mero hecho de mantener dichos activos en custodia bajo el nombre del custodio por cuenta del cliente. Así, la custodia engloba tradicionalmente los dos casos siguientes: (i) para los activos materiales que pueden entregarse físicamente al custodio (por ejemplo, un cuadro o una obra de arte), el custodio debe estar en condiciones de controlar físicamente y recuperar los activos; y (ii) para los instrumentos financieros que pueden registrarse en una cuenta de instrumentos financieros, el custodio debe registrarlos debidamente en dicha cuenta abierta en los libros del custodio a nombre del cliente.[40]

La práctica de los criptoactivos ha roto esta dicotomía establecida y ha introducido la noción de custodia y salvaguardia en forma de tenencia y control *de los medios de acceso* a dichos activos mediante claves criptográficas privadas. Por ejemplo, las normas de MiCA sobre la criptocustodia vinculan -de forma un tanto ambigua- la custodia en primer lugar a la custodia de criptoactivos, que a su vez incluye la salvaguardia de los derechos de los clientes y la prevención de su reutilización.[41]

2.3. Propuestas internacionales para regular a los custodios de criptoactivos

A la luz de todos estos incidentes, los custodios de criptoactivos ya se han convertido en el punto de mira de los responsables de políticas internacionales, dando lugar a propuestas de políticas parcialmente superpuestas. Según las recomendaciones políticas del FSB[42], el

[40] Debe tenerse en cuenta que la custodia *lato sensu* incluye más deberes que se complementan entre sí y, en última instancia, garantizan la salvaguardia de los derechos de los clientes sobre los activos custodiados, como la segregación de activos, la protección contra la insolvencia. En las páginas siguientes nos detendremos en estos últimos temas por separado para ofrecer una visión detallada

[41] MiCA, art 70(1) en relación con 75(3).

[42] FSB, *Global Regulatory Framework for Crypto-Asset Activities* (Policy Paper, 17 de julio de 2023), https://www.fsb.org/wp-content/uploads/P170723-1.pdf, [ultimately consulta :9/02/2025]; FSB, *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final report* (Policy Paper, 17 de julio de 2023), https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-. supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/. [ultimately consulta 9/02/2025] (denominado en el cuadro 1 "FSB (2023)").

FMI[43] y la IOSCO[44] que abordan la custodia de criptoactivos, los custodios deben salvaguardar los activos confiados y los derechos de sus clientes contra la pérdida y el mal uso, especialmente en caso de insolvencia, y deben proporcionar controles adecuados, así como políticas de custodia operativa, cibernética y de minimización de riesgos. También deberán mantener registros correctos y actualizados que establezcan las tenencias de sus clientes. Asimismo, deberán separar los criptoactivos confiados de sus propios activos, mientras que los acuerdos de transferencia de titularidad y la reutilización de los activos de los clientes sólo se permitirán con el consentimiento expreso previo del cliente y una amplia información *previa*. Cuando la custodia se subcontrate, deben implementar salvaguardias similares y una gestión de riesgos adicional e informar a los clientes en consecuencia. Por lo tanto, el depositario deberá proporcionar transparencia en relación*, entre otras cosas,* con los derechos y obligaciones derivados del acuerdo de custodia, los acuerdos de salvaguarda, cualquier externalización, cualquier uso de cuentas ómnibus, la reutilización respectiva de los activos de los clientes, así como todos los demás riesgos relacionados.

Finalmente, hay que destacar que los CASP multifuncionales que ofrezcan custodia deberán identificar, revelar y gestionar cualquier conflicto de intereses, y estarán sujetos a una separación obligatoria de funciones o incluso a la desagregación de líneas de negocio. El FMI y la OICV establecen requisitos sobre la custodia y segregación de los fondos de los clientes; además, los custodios deben disponer de fondos propios adicionales o participar en sistemas de garantía para compensar a los clientes en caso de pérdida o robo de activos, o de aseguramiento de estos. El FMI recomienda además la adopción de un plan eficaz de liquidación, mientras que la OICV sugiere conciliaciones adecuadas y frecuentes dentro y fuera de la cadena.

Todo esto, hace pensar que el legislador carece de experiencia en el mercado de las cripto, ya que se recuerda a la directiva MIFID respecto a la transparencia en la provision de información y en los riesgos asociados.

---

[43] FMI, *Elements of Effective Policies for Crypto Assets* (Policy Paper, febrero de 2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements- of- Effective-Policies-for-Crypto-Assets-530092, [ultimately 9/02/2025/ (denominado en el cuadro 1 "FMI (2023)"); FMI, "*Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets*" (Política) (Policy Paper, septiembre 2022),

[44] IOSCO, *Informe final, Recomendaciones políticas para los mercados de criptomonedas y activos digitales*. Documento Política,16 noviembre 2023) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf [ultimately consulta 9/02/2025]

3. LA PROPUESTA EUROPEA DE REGULACION PARA LOS CRIPTOACTIVOS

3.1. Introducción

El escenario financiero global ha sufrido cambios profundos con la aparición de las criptomonedas, lo que ha traído consigo oportunidades únicas y desafíos regulatorios importantes. En este contexto, la Unión Europea ha notado la importancia de establecer un marco normativo sólido y específico para abordar las complejidades de estos nuevos instrumentos financieros. A pesar de ser innovadora y avanzada, la Directiva sobre Mercados de Instrumentos Financieros (MiFID II) no logra cubrir completamente las particularidades de las criptomonedas como se mencionó previamente. Por esta razón, surge el Reglamento sobre Mercados de Criptomonedas (MiCA), una iniciativa de la Comisión Europea incluida en la propuesta COM (2020)593, que pone un énfasis especial en la custodia de criptoactivos. La creación del MiCA tiene lugar en un entorno donde las criptomonedas como Bitcoin y Ethereum están experimentando un crecimiento rápido y una mayor aceptación, respaldadas por la tecnología blockchain. La popularidad de estos activos digitales, junto con su extrema volatilidad y su naturaleza descentralizada, planteó numerosos desafíos a los reguladores. La falta de armonización regulatoria en Europa, donde cada Estado miembro aplicaba sus propias normativas generando una incertidumbre significativa tanto para los participantes del mercado como para los inversores. Era evidente que se necesitaba un marco regulador coherente que ofreciera claridad y consistencia, fomentando la innovación al mismo tiempo que protegía los intereses de los inversores y mantenía la estabilidad del mercado.9

La propuesta de MiCA en septiembre de 2020 representó un avance importante para la Unión Europea. Surgió como parte de un conjunto más amplio de medidas financieras digitales, con el propósito de asegurar que Europa adoptara la innovación tecnológica sin comprometer la estabilidad financiera ni la protección del inversor. Tras su presentación, la Comisión Europea abrió una consulta pública para recabar opiniones de diversas partes interesadas, incluidos reguladores nacionales, entidades financieras, proveedores de servicios relacionados con criptomonedas e inversionistas. Este proceso de retroalimentación resultó fundamental para perfeccionar la propuesta y garantizar que respondiera efectivamente a las demandas del mercado.

Durante los años 2021 y 2022, la propuesta de MiCA fue objeto de intensos debates y revisiones en el Parlamento Europeo y el Consejo de la Unión Europea. Estas discusiones

se enfocaron en lograr un equilibrio delicado entre promover la innovación y asegurar una protección adecuada para los inversionistas. Finalmente, en 2023, MiCA fue formalmente aprobado, representando un hito significativo en la regulación de activos digitales en Europa.

La implementación de MiCA se llevó a cabo en etapas. La primera fase, que comenzó en 2023, se concentró en establecer requisitos para el registro y supervisión de los proveedores que ofrecen servicios relacionados con criptomonedas.

La siguiente etapa, programada para el año 2024, introdujo normativas más estrictas en cuanto a la custodia de criptomonedas, incluyendo medidas de seguridad avanzadas y requisitos de segregación de activos. El Reglamento (UE) 2023/1114, conocido como MICA (Markets in Crypto-Assets), constituye una intervención normativa crucial en el ámbito de los criptoactivos dentro de la Unión Europea. Este reglamento, adoptado el 31 de mayo de 2023, se posiciona como un pilar esencial para la regulación de un sector que, hoy en día, ha operado con una considerable ausencia de normativas específicas, generando incertidumbres y riesgos tanto para los actores del mercado como para los consumidores. Con la entrada en vigor de diversas disposiciones a lo largo de 2024, se espera una transformación significativa en el paisaje regulatorio de los criptoactivos.

3.2. Alcance de las reglas de custodia de MiCA

El Reglamento MiCA está diseñado como un marco normativo integral que intenta cerrar las lagunas legales en la regulación de los criptoactivos dentro de la Unión Europea. Su estructura está concebida para abordar de manera sistemática las diferentes dimensiones de este mercado, proporcionando reglas tanto para los emisores de criptoactivos como para los proveedores de servicios relacionados.

El reglamento comienza definiendo su alcance y estableciendo las bases conceptuales necesarias para su interpretación. En este sentido, delimita los criptoactivos que regula, dividiéndolos en tres categorías principales: tokens referenciados a activos (ARTs), tokens de dinero electrónico (EMTs) y otros criptoactivos no cubiertos por normativas existentes. Este apartado también identifica excepciones específicas, aclarando dónde no resulta aplicable MiCA debido a la existencia de marcos regulatorios ya establecidos, como en el caso de instrumentos financieros o depósitos estructurados.

A lo largo del texto, MiCA establece las obligaciones fundamentales para los emisores de criptoactivos, exigiendo la elaboración de un libro blanco detallado, salvo en los casos expresamente exentos. Por su parte, los proveedores de servicios de criptoactivos (CASPs) están sujetos a requisitos estrictos en cuanto a autorización, gestión de riesgos y transparencia, con ciertas excepciones en función del tipo de servicio ofrecido y de los activos involucrados.

Otro punto clave en la estructura del reglamento es la regulación de la custodia de activos digitales. Aquí, MiCA introduce reglas específicas para proteger los intereses de los titulares de criptoactivos, aunque su interacción con otras normativas, como la Directiva de Gestores de Fondos de Inversión Alternativos (GFIA), genera interesantes cuestiones sobre el alcance y la superposición de las distintas obligaciones legales.

Con esta base, MiCA establece un marco sólido para abordar los aspectos fundamentales del ecosistema de criptoactivos, dejando también margen para el debate en áreas donde su aplicación plantea desafíos prácticos o conceptuales.

Como breve recordatorio, El Artículo 4(3) de MiCA exime a una serie de tipos de tokens de las obligaciones de libro blanco establecidas en el Título II de MiCA. El Artículo 4(5) de MiCA proporciona la exención análoga con respecto a los servicios de criptoactivos en relación con estos tipos de tokens; en todos estos casos, el CASP está exento del Título V de MiCA.

Emergen cuestiones de delimitación en relación con dos aspectos:; el alcance de la aplicación de MiCA a aplicaciones completamente descentralizadas; y la definición de MiCA de "custodia".

MiCA es un ejercicio de relleno de brechas que se centra en los criptoactivos. No se aplica donde los servicios financieros ya están regulados (cf. Artículo 2(4) de MiCA). A su vez, las reglas de MiCA no se aplican donde un activo digital califica como un instrumento financiero o un depósito estructurado, por nombrar solo dos de varios ejemplos. A la luz de lo anterior, el alcance de MiCA se limita a EMT, ARTs y "otros criptoactivos" dentro del alcance de MiCA que no califican como EMT y ARTs.[45]

[45] Véase el art. 4(1) MiCA.

Tenga en cuenta que la lista de exenciones de MiCA no menciona la gestión de carteras colectivas[46]. A su vez, para los fondos de inversión, a veces solo se aplican las reglas para fondos que se invierten en instrumentos financieros, a veces solo se aplican las reglas para fondos de inversión alternativos y a veces se aplican las reglas de MiCA además de las reglas sobre fondos de inversión alternativos. En particular, bajo la ley financiera de la UE, la custodia de activos en nombre de fondos de inversión alternativos está sujeta a reglas particulares especificadas en el Artículo 21 de la GFIA.[47], lo que puede generar conflictos normativos o duplicidad de requisitos. Esto se traduce en un desafío práctico, ya que los proveedores de servicios deben garantizar el cumplimiento tanto de MiCA como de otros marcos regulatorios aplicables, dependiendo de la naturaleza del activo y del servicio.

3.3. ¿Aplicaciones completamente descentralizadas como CASP?

Para profundizar más en detalle lo expuesto en el capítulo 1, resulta pertinente analizar cómo la naturaleza descentralizada de ciertos criptoactivos, como Bitcoin, plantea importantes desafíos regulatorios. Uno de los problemas centrales que subyace en la regulación de estos activos es la dificultad de identificar un emisor único de tokens. Esta característica intrínseca de Bitcoin, que no cuenta con una autoridad centralizada ni un emisor identificable, contrasta con los principios tradicionales de las normativas financieras y crea un vacío que las regulaciones, como MiCA, intentan abordar de forma limitada. De acuerdo con el Considerando 22, donde los criptoactivos no tengan un emisor identificable, no deberían estar dentro del alcance del Título II, III o IV de [MiCA][48]. Sin embargo, los

[46] A modo de ejemplo, un fondo de inversión que opere con Bitcoin podría encontrarse en un escenario complejo respecto a qué normativa debe aplicarse. A veces, solo se aplican las reglas para fondos que invierten en instrumentos financieros, como establece la Directiva UCITS, pero dado que Bitcoin no califica como instrumento financiero según el TJUE, no quedaría cubierto por dichas reglas. En otras ocasiones, los fondos de inversión alternativos (GFIA) son los que rigen, pero en ciertos casos específicos las disposiciones de MiCA podrían añadirse a las reglas de los fondos de inversión alternativos.

[47] En particular, bajo la ley financiera de la UE, la custodia de activos en nombre de fondos de inversión alternativos, incluyendo Bitcoin y otros criptoactivos, está sujeta a reglas particulares especificadas en el Artículo 21 de la GFIA. El TJUE ya ha señalado en casos previos que, al no tratarse de un instrumento financiero en el sentido estricto del derecho europeo, Bitcoin y otros criptoactivos deben analizarse bajo marcos específicos como MiCA. Por ejemplo, un custodio que gestione Bitcoin para un fondo de inversión alternativo deberá tener en cuenta tanto las reglas de custodia bajo MiCA como las derivadas de la GFIA en lo que respecta a la seguridad y segregación de activos.

[48] La Sentencia del Tribunal de Justicia de la Unión Europea Nº 326/2019 fue una de las primeras en pronunciarse sobre la naturaleza de Bitcoin, estableciendo que no puede ser considerado un "instrumento financiero" en los términos de la legislación europea. Este fallo refuerza el argumento de que Bitcoin opera fuera de los marcos tradicionales de regulación debido a su carácter descentralizado, lo que complica su inclusión dentro de las categorías normativas existentes. En línea con esto, MiCA, a través de su Considerando

proveedores de servicios de criptoactivos que presten servicios en relación con tales criptoactivos deberían estar cubiertos por MiCA. El Considerando 22, por lo tanto, aclara que los CASP deben cumplir con el Título V de MiCA incluso cuando los Títulos II, III y IV de MiCA no se apliquen[49]. Aplaudimos esta aclaración ya que, con respecto a los custodios de criptoactivos, hace innecesaria la difícil decisión de qué constituye "aplicaciones parcialmente" descentralizadas en contraste con "aplicaciones completamente descentralizadas". Esto significa que, para los tokens emitidos por aplicaciones parcial y completamente descentralizadas, se aplican las reglas de CASP si se proporciona un servicio de criptoactivos.

Más allá de la calificación y el grado de descentralización del emisor del token, si el Título V se aplica a los proveedores de custodia completamente descentralizados requiere una consideración adicional. Desde el principio, la respuesta parece ser afirmativa, ya que el Título V se basa en actividades. Sin embargo, la definición de un CASP en el Artículo 3(1)(15) de MiCA establece que "proveedor de servicios de criptoactivos" significa "una persona jurídica u otra entidad cuya ocupación o negocio es la prestación de uno o más servicios de criptoactivos a clientes de manera profesional". Esta noción es confirmada por el Considerando 22 que excluye del alcance de MiCA la prestación de servicios de criptoactivos de manera completamente descentralizada sin ningún intermediario.

En base a eso, las aplicaciones completamente descentralizadas desafían la definición de CASP en dos aspectos. Primero, puede faltar el requisito de una "persona jurídica" o "entidad". Segundo, dado que los contratos inteligentes realizan servicios, podríamos cuestionar si el servicio es proporcionado por una persona y/o de manera profesional. MiCA no define "entidad", pero el entendimiento general como "una tarea o proyecto, especialmente uno que es importante y/o difícil," similar a un emprendimiento, cubriría proyectos de criptoactivos descentralizados. Respecto al segundo elemento, es decir, la cuestión de si el servicio es proporcionado por contratos inteligentes o personas, argumentamos que esto no es un criterio de relevancia para el alcance de MiCA (es decir, MiCA se aplica independientemente de si el servicio es realizado por código o humanos y

22, reconoce explícitamente que los criptoactivos que no tengan un emisor identificable, como Bitcoin, no deberían estar sujetos a las obligaciones establecidas en los Títulos II, III y IV del reglamento.

[49] Si un CASP proporciona servicios de custodia para Bitcoin, no están obligados por el Título II, pero sí por el Título V, ya que estas obligaciones se aplican a los proveedores de servicios, independientemente de si el criptoactivo tiene o no un emisor identificable.

que la prestación de servicios por contratos inteligentes es una de las características distintivas de la industria de criptoactivos). Sin embargo, las autoridades nacionales competentes tienen dificultades para identificar a alguien para cumplir con la regulación si el servicio es proporcionado por una aplicación que está completamente dispersa, con múltiples partes no relacionadas contribuyendo, y con nodos de Bitcoin funcionando como el arquetipo. Por esa razón, sostenemos que siempre que alguien controle una aplicación, ya sea por medios legales o fácticos, ese "alguien" es el CASP para los propósitos del Título V de MiCA[50]. Segundo, el término "de manera profesional" excluye proyectos meramente de *hobby*. En la ley financiera de la UE, en general, "de manera profesional" se materializa si el servicio se proporciona de manera permanente y el proveedor (es decir, la plataforma) busca clientes mediante comunicación orientada al cliente. Este requisito es cumplido por muchas soluciones de custodia de criptoactivos.[51]

A continuación, intentamos determinar si los proveedores de servicios asumen obligaciones de custodia de criptoactivos estipulando explícitamente que custodian los criptoactivos de los clientes, almacenan claves privadas, proporcionan carteras (de custodia), salvaguardan o custodian activos, o aseguran y protegen activos u otras expresiones similares.

3.4. Control sobre claves criptográficas como un criterio central de "custodia"

El Artículo 3(1)(17) de MiCA establece que la prestación de "custodia y administración de criptoactivos en nombre de los clientes" significa la custodia o el control, en nombre de los clientes, de criptoactivos o de los medios de acceso a dichos criptoactivos, donde sea aplicable en la forma de claves criptográficas privadas.

Surgen dos cuestiones a partir de este texto legislativo. Primero, MiCA aclara que los criptoactivos pueden ser mantenidos en custodia, un asunto que se discutió ampliamente antes de MiCA. Segundo, dado que un criptoactivo es intangible, y su existencia depende del reconocimiento por parte de los nodos en el DLT, define que la custodia "significa la custodia o el control ... de los medios de acceso a dichos criptoactivos, donde sea aplicable en la forma de claves criptográficas privadas"[52]. Lo anterior se complementa con el

[50] Para un análisis detallado, véase Zetzsche,Woxholth, "EU Regulation of Crypto-assets" Cambridge University Press, Cambridge, 2024.

[51] Considerandos 12, 30 MiFID

[52] Art. 3(1)(17) MiCA

Considerando 83, que establece que el acuerdo de custodia debe "especificar," entre otras cosas, la naturaleza del servicio proporcionado, que podría incluir la tenencia de criptoactivos pertenecientes a clientes o los medios de acceso a dichos criptoactivos, en cuyo caso el cliente podría mantener el control de los criptoactivos en custodia. Alternativamente, los criptoactivos o los medios de acceso a ellos podrían ser transferidos al control total del proveedor de servicios de criptoactivos.[53]

Nos preguntamos qué significa "'tenencia" de un criptoactivo para una clase de activos donde la existencia del criptoactivo depende del procesamiento del mismo código por múltiples nodos, por lo que el token en sí mismo está potencialmente almacenado en múltiples servidores simultáneamente, y solo se conserva la clave de acceso para el titular del criptoactivo. Esto desvía la atención de la custodia a la segunda característica mencionada en el Artículo 3(1)(17) de MiCA: control de los medios de acceso a dichos criptoactivos.

Sin embargo, MiCA no especifica exactamente qué implica "control" sobre las claves. Esta es una característica importante cuando se trata de definir qué proveedores de carteras caen bajo la definición del Artículo 3(1)(17) de MiCA, delineando así a los proveedores que ofrecen servicios de carteras de custodia de aquellos que ofrecen una cartera autogestionada o no custodiada fuera del alcance de MiCA. Esta distinción es crucial dado que la práctica ha desarrollado un espectro completo de soluciones de carteras custodiadas, no custodiadas e intermedias.[54]

Por un lado, están las soluciones custodiadas donde los clientes no tienen acceso directo ni a los criptoactivos ni a las claves privadas. El custodio genera pares de claves públicas-privadas (o carteras) nuevas para los criptoactivos que aceptan mantener en custodia. La custodia y recuperación de las claves y los activos aquí están vinculadas al custodio. Y en el otro lado están las soluciones de custodia donde solo el cliente tiene posesión de las claves (la llamada autogestión). Para estos casos, los considerandos de MiCA

---

53 Woxholth,Jannik,Zetzsche,D.,Buckley,R,Arner, "Competing Claims to Cryptoassets", Universidad de Hong Kong, 2023 [ultimately consulta 9/02/2025]

54 Para una visión general cf. Goforth,C, Guseva,Y, "Regulation of Cryptoassets, American Casebook Series", 2nd ed., West Academic Publishing 2022, pp. 760-781,790
De Filippi, Primavera and Wright, Aaron, Blockchain and the Law: the Rule of Code, Harvard University Press, Harvard, 2018.pp. 14-16, 20-29.Small,S, "Bitcoin: The Napster of Currency", Houston Journal of International Law, 2015, 37, 2, pp. 588 y ss.; Maume,P,Maute,LFromberger,M,"The Law of Crypto Assets", *Bloomsbury*,2022.pp. 6-10; Kaal,W,Howe,H, "Custody of digital assets", *Jurimetrics*, 2023, vol.63, 2, pp. 169-195.

aclaran que el proveedor de servicios está fuera de la definición de custodia, y por lo tanto no proporciona un servicio de criptoactivos bajo MiCA.[55]

Los usuarios generarán y controlarán sus propios pares de claves para mantener criptoactivos. Esto generalmente ocurre a través de una cartera jerárquica determinista con una semilla codificada como una frase mnemotécnica[56], donde la semilla es la clave maestra, generada aleatoriamente durante la inicialización de la cartera por el usuario, y este último necesita hacer una copia de seguridad. Si el usuario pierde acceso a su cartera y a la semilla, sus activos se pierden por completo.[57]

Por esa razón, las soluciones de custodia intermedia comparten el control de las claves de alguna manera entre el usuario y el proveedor de la cartera. Donde la autogestión se define por el control exclusivo de las claves por parte del usuario, estos casos son limítrofes y deben evaluarse según la manera en que se ejerce el control sobre la clave.

Esto resulta en una taxonomía de soluciones de custodia intermedia:

1. Proveedores de carteras con soluciones intermedias que asignan el control de las claves al cliente, mientras que la clave maestra es respaldada por el proveedor de la cartera, pertenecen al primer grupo de soluciones custodiadas, donde el control reside eventualmente con los custodios. Por ejemplo, en el caso de Ledger Recover, la cartera divide la semilla del usuario en tres fragmentos, que se envían a tres entidades para fines de respaldo. Las claves pueden ser generadas por el usuario en la fase de inicialización de la cartera, de modo que "nunca abandonan el dispositivo de la cartera"; de hecho, las claves también pueden ser regeneradas a partir de estos respaldos cuando sea necesario. En estos casos, la cartera asigna cierto control de las claves a sus usuarios, pero el control no es exclusivo, por lo que el proveedor de la

[55] Ejemplos de proveedores de monederos custodiados son CEFFU, Coinbase Custody, Taurus, BitGo, Seba Bank; proveedores de monederos no custodiados son Trezor, Atomic Wallet, MetaMask; soluciones intermedias son Ledger Recover, Zengo wallet, Casa 2-of-3 multisig wallet.

[56] El monedero es determinista porque la misma clave maestra-semilla siempre producirá la misma secuencia de claves, incluso cuando se importe a nuevos monederos. La semilla es un mecanismo de recuperación. La mnemotecnia permite conservar o recuperar los datos de acceso al criptoactivo (las "claves"). Fuente: Capítulo 5. Wallets en Andreas ,M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain", 2nd ed., *O'Reilly Media* ,2017.[ultimately consulta: 9/02/2025]

[57]Buterin,V, "Why we need wide adoption of social recovery wallets",2021 https://vitalik.ca/general/2021/01/11/recovery.html [ultimately consulta 9/02/2025].

cartera tiene la capacidad de acceder (y por lo tanto potencialmente controlar) las claves, mientras que los usuarios (necesitan) confiar en que el proveedor de la cartera no abusará de ese poder.[58]

2. El segundo grupo de soluciones intermedias, donde el control reside en gran medida con el cliente, incluye casos de carteras de firmas múltiples ("multisig"), uso compartido de claves u otras tecnologías similares. Estas tecnologías crean múltiples claves o partes de claves que pueden ser mantenidas por diferentes personas, mientras que se requiere un umbral mínimo de estas claves o partes de claves para realizar cualquier transacción respecto a x criptoactivos. En nuestro caso, el proveedor de la cartera y el cliente mantienen diferentes claves o partes de claves sobre los mismos activos. Consideramos una situación donde ni las clave(s) o parte(s) de clave(s) mantenidas por el cliente, ni las clave(s) o parte(s) de clave(s) mantenidas por el proveedor de servicios son suficientes para iniciar una transacción. Por lo tanto, para que ocurra cualquier transacción, la colaboración y "co-aprobación" del proveedor de la cartera y el cliente son necesarias. Un ejemplo de esto es la cartera Zengo.[59]
3. Respecto al tercer grupo intermedio, estos abarcan casos de carteras multisig, uso compartido de claves y tecnologías similares donde el cliente mantiene solo el umbral mínimo de claves o partes de claves necesarias para realizar una transacción por su cuenta. El proveedor de la cartera mantiene algunas clave(s) o parte(s) de clave(s) que solas no son suficientes para ninguna transacción y no tienen acceso a las clave(s) o parte(s) de clave(s) de los clientes. Así, las clave(s) o parte(s) de clave(s) del proveedor de la cartera se mantendrán principalmente para fines de respaldo en caso de que los clientes pierdan algunas de sus clave(s) o parte(s) de clave(s).[60]

---

[58] Beimer,A., "Esquemas de compartición de secretos: A survey, International" *conference on coding y cryptolo,* 2011,https://www.researchgate.net/profile/Amos-Beimel/publication/220776045_SecretSharing_Schemes_A_Survey/links/09e41513f14a20f236000000/Secr t-Sharing- Schemes-A-Survey.pdf [consulta: 27 mar 2024], pp. 2-3; Aumasson,J-P.,Hamelink,A., Shlomovits,O,. "A survey of ECDSA threshold signing, Cryptology ePrint Archive", 2020, https://eprint.iacr.org/2020/1390.pdf, pp. 1-7, [ultimately consulta: 9/02/2025]

[59] En palabras sencillas, dependiendo de la configuración y la tecnología del monedero, nos encontramos con monederos con múltiples claves o claves compartidas en los que ni el proveedor del monedero ni el cliente poseen por sí solos el umbral necesario de claves o claves compartidas para iniciar una transacción y necesitan coordinarse

[60] Un ejemplo es el monedero multisig 2-de-3 de Casa con dos claves de hardware. Véase Casa, "Choosing your 3-key vault setup", https://support.keys.casa/hc/en- us/articles/360045419111-Choosing-Your-Basic-Multisig-Setup, [ultimately consulta 9/02/2025](donde se afirma que "Dos claves de hardware, preferiblemente

Trazamos la línea aquí basándonos en los riesgos que enfrentan los clientes que dependen de la solución de custodia: donde los clientes enfrentan el riesgo de que los medios de acceso puedan ser robados u obtenidos mediante "trabajos internos" por partes o personas no autorizadas para los activos, existen los riesgos típicos de custodia abordados por el Título V de MiCA. En estos casos, las reglas de MiCA (deben) aplicarse. A su vez, sostenemos que MiCA se aplica al primer grupo de soluciones de custodia intermedias donde todos los datos relevantes de acceso (es decir, donde todas las claves son meros conjuntos de datos) pueden ser obtenidos del personal, servidores y algoritmos del proveedor de servicios, pero no al segundo o tercer grupo intermedio, ya que aquí ninguna conducta por parte del proveedor de la cartera o su personal por sí sola es suficiente para obtener el control sobre los activos.

3.5. Las Reglas de MiCa sobre custodios de criptoactivos

El Título V del Reglamento MiCA establece disposiciones específicas para los Proveedores de Servicios de Criptoactivos (CASP), abarcando una amplia gama de servicios relacionados con criptoactivos que se definen en el Artículo 3(1)(16) de MiCA. Dentro de estos servicios se incluye, entre otros, la "provisión de custodia y administración de criptoactivos en nombre de clientes" (Artículo 3(1)(16)(a) de MiCA). Aunque la enumeración de servicios no es exhaustiva (por ejemplo, no aborda expresamente el préstamo o la participación de criptoactivos), MiCA no exige que las actividades reguladas constituyan la actividad principal o exclusiva del proveedor. En este sentido, basta con que el CASP ofrezca, entre otras, la custodia y administración de criptoactivos en nombre de clientes para que le resulten aplicables las normas pertinentes.

Para prestar este tipo de servicios, los CASP deben obtener una autorización de conformidad con lo dispuesto en el Capítulo 1 del Título V de MiCA. Dicha autorización puede ser específica para un servicio de criptoactivos o bien una ampliación de una licencia existente, como la de una institución de crédito, una entidad de dinero electrónico, un

de distintos fabricantes (Ledger, Trezor, Coldcard, etc.), una clave de recuperación de Casa (en poder de Casa para emergencias en caso de que le ocurra algo a una de las otras claves"); "*Casa Terms and Condition*s", https://casa.io/terms-of-service, Consulta: 27 mar 2024 (en el que se establece que "Usted reconoce y acepta que si decide autorizar a Casa a controlar una clave criptográfica creada por usted a través de los Servicios (una "Clave de recuperación"), (i) Casa tendrá el control único y exclusivo sobre dicha Clave de recuperación. [...] Usted reconoce además que los Servicios pueden requerir la transmisión de múltiples claves criptográficas a una Bolsa para acceder a su moneda digital o virtual o a sus activos, y que la Clave de Recuperación por sí sola puede ser insuficiente para dicho acceso sin al menos una (1) o más Claves Privadas")

proveedor de servicios de pago, una empresa de inversión regulada por MiFID o un gestor de fondos de inversión.

Adicionalmente, el Capítulo 2 del Título V de MiCA introduce normas generales aplicables a todos los CASP, mientras que el Capítulo 3 regula actividades específicas sujetas a requisitos particulares. Tras analizar el ámbito de aplicación del Título V en relación con los servicios de custodia, se expondrán los requisitos operativos más relevantes.

3.5.1. Principio de concesión de licencias

En el caso de los CASP que no posean una licencia pertinente en virtud de la legislación financiera de la UE, los arts. 59, 61 y ss. MiCA prevén un requisito de autorización completo. Esta autorización es importante para los nuevos proveedores de servicios que deseen prestar servicios a los GFIA como delegados en relación con la transmisión y recepción de órdenes, la gestión de carteras y el asesoramiento.[61]

Los gestores de fondos, las entidades de dinero electrónico y de crédito y las empresas MiFID (así como otros intermediarios autorizados) pueden obtener el derecho a prestar servicios de criptoactivos mediante notificación a sus respectivas ANC. Estas entidades necesitan entregar la información relevante para ampliar la autorización especificada en el Art. 60(9) MiCA, 40 días antes del inicio del servicio a su ANC. Para evitar la repetición de documentación y las dobles revisiones, los CASP que sean titulares de una licencia en virtud de la legislación financiera de la UE no necesitan presentar ninguna información que ya hayan entregado como parte de su proceso de autorización anterior si dicha información es idéntica, pero deben declarar que este es el caso en su notificación.[62]

En resumen, el Reglamento MiCA introduce un modelo de autorización más flexible y adaptado a las necesidades del mercado de criptoactivos. Permite aprovechar autorizaciones previas y acelera el proceso para entidades ya reguladas, evitando duplicidades. Al contrario, MiFID II adopta un enfoque más rígido y tradicional, con mayores costos y plazos asociados. La flexibilidad y la agilidad de MiCA representan una innovación en el

[61] Art. 20(1), 6(4)(b) GFIA.

[62] La ANC dispone entonces de 20 días para requerir en un solo trámite información adicional cuando la notificación esté incompleta, y fijar un nuevo plazo no superior a 20 días que retrasa la expiración del plazo de 40 días. Las solicitudes posteriores no amplían el plazo.

ámbito regulatorio, pero también plantean desafíos para garantizar un nivel homogéneo de supervisión en todos los Estados miembros.

3.5.2. Pasaporte UE

Los CASP que reciban autorización podrán prestar servicios de criptoactivos en toda la Unión, ya sea mediante el derecho de establecimiento, incluso a través de una sucursal, o mediante la libre prestación de servicios. No se exigirá a los CASP que presten servicios de criptoactivos con carácter transfronterizo que dispongan de una sucursal física en el territorio de un Estado miembro de acogida.[63]

MiCA, como un reglamento (en lugar de una directiva), es de aplicación directa en toda la Unión Europea sin necesidad de transposición. Esto elimina las discrepancias nacionales y garantiza una armonización completa en el tratamiento de los proveedores de servicios de criptoactivos (CASP) y los emisores de criptoactivos. Esta uniformidad es crucial en un mercado digital como el de los criptoactivos, donde la interoperabilidad y la confianza transfronteriza son esenciales. El legislador europeo ha reconocido la necesidad de un marco único para fomentar la competitividad de la UE en el ámbito global de los criptoactivos.

3.5.3. Requisitos generales y de funcionamiento

El Título V MiCA regula principalmente las relaciones entre los CASP y los clientes (y, en algunos casos, los emisores de criptoactivos), por lo que aplica una perspectiva reguladora similar a la de las empresas de inversión. El Título V Capítulo 2 MiCA estipula las condiciones *generales* de funcionamiento aplicables a todos los CASP. Los más importantes de estos requisitos para los criptocustodios incluyen los deberes fiduciarios (arts. 66 y 72 MiCA), las delegaciones y la externalización (art. 73 MiCA), y la recuperación de activos y la continuidad de la actividad (art. 74 MiCA).

a) Deberes fiduciarios (arts. 66 y 72 MiCA) Equivalente a disposiciones similares de la legislación financiera de la UE, el art. 66(MiCA establece que los CASP son fiduciarios: Los CASP "actuarán con honestidad, imparcialidad y profesionalidad en el mejor interés de sus clientes y posibles clientes". [64]

[63] Art. 65 MiCA

[64] Véase Art. 24 MiFID, 25 OICVM, 21 (10) GFIA.

Esta disposición sustenta una serie de requisitos sobre imparcialidad, transparencia y gestión de conflictos de intereses, que siguen el principio de que los intereses de los clientes deben ser primordiales, a menos que los clientes hayan sido informados y hayan dado su consentimiento explícito a ser tratados de manera desventajosa.

Los deberes fiduciarios tienen, por un lado, un efecto armonizador que alinea la posición de los CASP con la de otros intermediarios fuera de balance en el ámbito de las finanzas. La MiCA aclara sin lugar a duda que los CASP no deben utilizar los activos de los clientes por cuenta propia. Por otro lado, establece límites a los modelos de negocio de criptomonedas que dan lugar a transferencias de valor de los clientes a los CASP, como eran frecuentes en el momento álgido del Crypto Winter.

b) Subcontratación (Art. 73 MiCA)

El art. 73 MiCA sobre externalización se inspira en el art. 16(5) MiFID y Art. 20 de la Directiva sobre fondos de inversión alternativos y sus respectivas normas de desarrollo. La finalidad del art.16(5) MiFID es garantizar la eficacia de los requisitos de autorización y supervisión financiera incluso cuando los CASP autorizados recurran a otros proveedores de servicios, potencialmente no autorizados.[65]

Los CASP "que subcontraten servicios o actividades a terceros para el desempeño de funciones operativas adoptarán todas las medidas razonables para evitar riesgos operativos adicionales. Seguirán siendo plenamente responsables del cumplimiento de todas sus obligaciones en virtud del título V de la MiCA". Los CASP que participen en la externalización deben asegurarse de que ésta no: (1) dé lugar a la delegación de su responsabilidad; (2) altere la relación entre ellos y sus clientes, ni sus obligaciones para con éstos; y (3) altere las condiciones de su autorización. Una vez más, los acontecimientos ocurridos durante el Crypto Winter explican la introducción de tales normas: muchos CASP carecían de experiencia en servicios financieros y eran incapaces de gestionar los riesgos operativos de sus aplicaciones DeFi y de las entidades relacionadas con ellas. Estas normas

[65] Véase Art. 13-15 Directiva 2006/73/CE de la Comisión, de 10 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2004/39/CE del Parlamento Europeo y del Consejo.

de externalización garantizan que la solidez institucional del principio de autorización no pueda eludirse por la vía de la delegación.[66]

La cuestión central en relación con el art. 73 MiCA es establecer cuándo un servicio en el que se confía es un *tercero* (desde la perspectiva de MiCA) y cuándo ese tercero realiza *funciones operativas*.[67] En lo que respecta a la custodia como servicio de criptoactivos, para ser considerado delegado, ese tercero debe proporcionar partes materiales de los servicios de custodia. Dado que el núcleo de la custodia es el control de los medios de acceso, entre los ejemplos de funciones operativas se incluyen el almacenamiento externo de claves privadas, la participación en la nueva generación de claves perdidas o claves compartidas, o la dependencia de un subcustodio con puentes para conectarse a criptoactivos distintos de aquellos a los que el custodio puede acceder a través de sus propios puentes. Las empresas desarrolladoras de software se dedican al desarrollo de código, alojamiento y gestión de crisis (en respuesta a ciberataques o fallos de funcionamiento); cuando estos servicios conllevan el acceso temporal a las claves privadas o su almacenamiento, estas empresas actúan como delegadas de la CASP y, en consecuencia, están sujetas indirectamente a regulación; en el caso de los acuerdos de subcustodia, están sujetas a regulación directa como CASP si la empresa está ubicada en la UE/EEE. Damos cuenta de esta evaluación de la misma manera que clasificamos las soluciones de custodia en general siempre que el proveedor de servicios pueda presentar un único punto de fallo que dé lugar a una pérdida potencial de activos, se aplica la MiCA.[68]

---

[66] Según la propuesta inicial de la Autoridad Europea de Valores y Mercados (AEVM), también deberán llevar registros detallados de los acuerdos de externalización y de los servicios y actividades externalizados. Cf. Documento de consulta de ESMA sobre estándares técnicos que especifican ciertos requisitos del Reglamento sobre Mercados de Criptoactivos (MiCA) - segundo documento de consulta, ESMA75-453128700-438, pp. 162, 171-172.

[67] Según la propuesta inicial de la AEVM, las DLT sin permiso se considerarán una forma de recurso de "bien común", mientras que el uso de una DLT con permiso operada por una empresa comercial probablemente se basará en contratos disponibles para productos de blockchain de "marca blanca"; en cuyo caso puede considerarse como un "proveedor tercero". Cf. ESMA Consultation Paper on Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper, ESMA75-453128700-438, p. 19. Esta calificación fomenta la externalización a aplicaciones que el proveedor no puede controlar ni supervisar, en particular si se considera junto con los privilegios que la AEVM prevé en materia de responsabilidad en estos casos.

[68] Para más detalles, véase Zetzsche,Woxholth, *EU Regulation of Crypto-assets*(de próxima publicación), Cap. 7. [ultimately Consulta : 9/02/2025]

c) Plan de enterramiento (Art. 74 MiCA)

El art. 74 de la MiCA exige a los proveedores de servicios de criptomoneda que ofrecen custodia que establezcan un plan de enterramiento, se traduce en un "plan adecuado para apoyar una liquidación ordenada de sus actividades con arreglo a la legislación nacional aplicable, incluida la continuidad o recuperación de cualquier actividad crítica realizada por dichos proveedores de servicios. Dicho plan deberá demostrar la capacidad de los proveedores de servicios de criptoactivos para llevar a cabo una liquidación ordenada sin causar un perjuicio económico indebido a sus clientes". Para ser eficaz, el plan debe ajustarse a la legislación nacional en materia de insolvencia. El hecho de que, hasta ahora, la legislación sobre insolvencia no esté armonizada en el ámbito de los criptoactivos, socava la eficacia de los planes de enterramiento para proteger los activos de los clientes.[69]

d) Custodia de los criptoactivos

Mientras que el Art. 75 MiCA establece normas específicas sobre la criptocustodia, una parte de la custodia, a saber, la custodia de criptoactivos, constituye el epígrafe del Art. 70 MiCA, y se asigna dentro de las normas generales aplicables a todos los CASP.

d.1) Custodia como custodia cualificada (art. 70(1) MiCA)

Aunque no todos los CASP proporcionan custodia en relación con criptoactivos, ya que también pueden custodiar "fondos" (es decir, equivalentes de efectivo) para facilitar los pagos, en los casos en los que se proporciona custodia *en relación con criptoactivos*, los arts. 70(1) y 75 MiCA se aplican conjuntamente. La MiCA regula la criptocustodia entonces como una forma cualificada de custodia bajo el Art. 70(1) MiCA, similar al Art. 21(8) MiCA que regula la custodia como un tipo cualificado de custodia para instrumentos financieros por cuenta de fondos de inversión alternativos.

En el ámbito de aplicación del Art. 70(1) MiCA no sólo caen criptocustodios, sino potencialmente también los gestores de carteras de criptomonedas, las bolsas de criptomonedas y los servicios de criptopréstamos y criptoapuestas que, aunque no entran en el ámbito de aplicación de la MiCA por su servicio principal, mantienen los activos de los clientes como servicio auxiliar. Como fuente de inspiración del legislador señalarse que según

[69] Art. 74 MiCA: Los CASP "dispondrán de un plan adecuado para apoyar una liquidación ordenada de sus actividades con arreglo a la legislación nacional aplicable.

los arts. 16(8) y (9) MiFID, los CASP "adoptarán las medidas adecuadas para salvaguardar los derechos de propiedad de los clientes, especialmente en caso de insolvencia [del CASP], y para impedir el uso de los criptoactivos de los clientes por cuenta propia". Así, en términos técnicos-jurídicos, la aplicación de MiCA plantea respuestas a problemas específicos y característicos de los criptoactivos. El primer requisito art.16(8)MiFID (protección en caso de insolvencia) depende de lo que sea necesario para proteger a los titulares de criptoactivos en virtud de las leyes de insolvencia aplicables en caso de insolvencia o quiebra de la aplicación DeFi .[70] El segundo requisito art.16(9) MiFID (prohibición del uso indebido de activos) responde a los abusos generalizados en los que los criptointermediarios (por ejemplo, FTX Exchange) trataban los activos de los clientes como propios, por ejemplo, para cubrir las pérdidas sufridas por criptoinversiones arriesgadas en otras partes de su criptoimperio (por ejemplo, Alameda, la filial de inversiones de FTX87) o para respaldar acuerdos de criptopréstamo en los que los activos de los clientes se agrupan y luego se transfieren a terceros acreedores.[71]

d.2) Contrato de custodia, política y procedimientos en virtud del art. 75 MiCA

El art. 75 MiCA sobre los servicios de custodia exige que los CASP residan en el mercado único europeo, y celebren un acuerdo con los clientes en el que se prescriban meticulosamente los detalles contractuales.[72]

Las estipulaciones más importantes aquí se refieren a la identidad de las partes (que puede ser difícil de averiguar en casos de sistemas totalmente descentralizados), la política de custodia, una descripción de los sistemas de seguridad del CASP, las tasas, costes y cargos que debe pagar el cliente y la legislación aplicable.[73] Con lo cual, el acuerdo esclarecería, en principio, estas cuestiones.

---

[70] Según la mayoría de las leyes de insolvencia, sólo las personas y las entidades pueden declararse insolventes, y no está claro si las solicitudes de DeFi pueden calificarse como una de las primeras

[71] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & van Ek, M. (2023), *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*, *Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies*, European Parliament, Luxembourg (2023): 23-27

[72] Art. 75 (1) MiCA. A diferencia del art. 21 (2) Gestor de fondos inversión alternativos, el art. 75 (1) MiCA no exige que este acuerdo sea escrito.

[73] Art. 75 (1) (a) a (g) MiCA.

Por otro lado, la política de custodia debe contener procedimientos destinados a garantizar la custodia o el control de los medios de acceso a los criptoactivos. Esta norma responde a los frecuentes incidentes de apropiación indebida de claves privadas administradas por custodios. Además, los derechos de los clientes sobre los criptoactivos, así como cualquier movimiento, modificación o creación de posiciones se registrará a nombre de cada cliente, mientras el cliente tenga derecho a recibir información sobre los asientos del registro. Esta norma permitirá una gestión transparente del ejercicio de los derechos de los clientes.[74]

Además, los CASP están obligados a proporcionar los procedimientos necesarios para la devolución de los criptoactivos a los clientes, así como una segregación (operativa) de los activos del cliente de los activos del CASP en el libro mayor distribuido. Esto garantizará, por ejemplo, que, en caso de insolvencia de la CASP, los activos del cliente permanezcan intactos.[75]

En particular, el art. 75(4) MiCA establece una disposición de derecho privado que obliga a la sustitución: los cambios en la DLT y otros acontecimientos que puedan afectar a los derechos de los clientes establecerán el derecho de los clientes "a cualquier criptoactivo o cualquier derecho de nueva creación sobre la base y en la medida de las posiciones del cliente en el momento en que se produzca dicho cambio o acontecimiento". Si bien estas disposiciones tienen por objeto proteger a los clientes del custodio, también exponen a los CASP al riesgo de responsabilidad por los acontecimientos que tengan lugar en la DLT y en los que los CASP puedan o no influir; téngase en cuenta que un CASP puede no tener ningún derecho de gobernanza en relación con la creación o modificación del token a través de la DLT. Si la DLT no asigna el derecho, o una parte de este, al token respectivo, es posible que nunca llegue a estar al alcance del custodio.

d.3) Responsabilidad del depositario

[74] Art. 75 (2), (4) MiCA. En el artículo 21, apartados 7 y 8, de la Directiva sobre fondos de inversión alternativos se prevé una supervisión equivalente de los flujos de tesorería y los activos en custodia de los FIA, con el fin de garantizar la protección de los inversores. 21 (7) y (8) de la Directiva FIA

[75] Art. 75 (7) MiCA. El artículo 21, apartado 8, letra a), inciso ii), de la Directiva sobre fondos de inversión alternativos prevé una segregación de activos equivalente y el registro de los activos de un FIA. 21 (8) (a) (ii) GFIA.

En este punto, al Reglamento MiCA desplaza el foco de atención hacia las responsabilidades del custodio. MiCA introduce una norma amplia en el Art. 75(8) MiCA: el custodio es responsable de la pérdida de los activos de sus clientes. Esta norma contrasta con los términos y condiciones de la mayoría de los proveedores de custodia de criptomonedas hasta la fecha, que suelen excluir totalmente la responsabilidad o limitarla al total de las comisiones cobradas de los clientes.[76] lo cual, constituye solo una fracción de las posibles pérdidas sufridas por los mismos. Además, esta responsabilidad legal cobra mayor relevancia, ya que no está condicionada a la existencia de culpabilidad o falta alguna por parte del depositario o de su personal.[77]

Sin embargo, un examen más detallado revela que la responsabilidad de los CASP está limitada en tres aspectos. En primer lugar, el CASP sólo es responsable de la pérdida de criptoactivos o de los medios de acceso a dichos activos. MiCA no prevé ningún otro daño que puedan sufrir los clientes, como la pérdida de oportunidades o daños a la reputación. En segundo lugar, la responsabilidad se limita a situaciones atribuibles a los CASP y bajo su control. En tercer lugar, la responsabilidad se limita al valor de mercado del criptoactivo perdido en el momento en que se produjo la pérdida.[78] En cualquier caso, el Art. 75(8) MiCA puede cambiar las reglas del juego en un entorno caracterizado por la falta de responsabilidad y resistencia.[79]

En cuanto a lo que constituye una pérdida, depende de la interpretación de la regla de sustitución y de la obligación de facilitar los derechos de sus clientes de forma más general: si el custodio decide no ampliar la custodia a los criptoactivos creados en el libro mayor a los que sus clientes tendrían derecho, la cuestión de si los clientes autorizaron debidamente al custodio a renunciar a cualquier derecho sobre el nuevo activo determinará si (una parte de) los activos se perdieron, de hecho (en lugar de cederse, cederse voluntariamente, donarse o

---

[76] Algunos ejemplos son: *"El Depositario no asume ninguna responsabilidad por cualquier pérdida o daño derivado del uso de su Cuenta y/o Servicios [...] por usted o cualquier tercero [...] con o sin su autorización.* Fuente: Términos y Condiciones de CEFFU, https://www.ceffu.com/legal/terms [ultimately consulta 9 /02/2025]

[77] Zetzsche, Dirk Andreas and Nikolakopoulou, Areti (2024), "Crypto Custody and Crypto Wallets – An Empirical Assessment" – (March 22, 2024), disponible online en SSRN: https://ssrn.com/abstract=4769396 or http://dx.doi.org/10.2139/ssrn.4769396. [ultima consulta 09.02.2025]

[78] Dado que la MiCA no se pronuncia sobre otras pérdidas, el régimen de responsabilidad aplicable es el de la legislación nacional

[79] Art. 75(8) MiCA. La disposición equivalente es el art. 21(12) GFIA y el art. 24 (1) OICVM.

cualquier otra cosa). La misma cuestión es relevante cuando el mecanismo de consenso y otros elementos de la DLT subyacente generan recompensas, beneficios u otros elementos de ingresos pasivos relacionados con los criptoactivos y el custodio se abstiene de cederlos a sus clientes; éstos podrían considerarse una parte del criptoactivo o una pérdida derivada de un derecho independiente del criptoactivo. En este contexto, el Art. 66 MiCA, que establece los deberes fiduciarios y la obligación de actuar en el mejor interés de sus clientes, proporcionará una directriz en ausencia de estipulaciones contractuales expresas y órdenes de los clientes.[80]

Más importante aún es determinar qué constituye un siniestro imputable al depositario, dado que la responsabilidad queda excluida cuando el siniestro no le es imputable. Un siniestro imputable es cualquier acontecimiento que se produzca en el ámbito de las operaciones del custodio y que éste controle o pueda controlar. En este caso, la cuestión central es lo que la ley supone que el custodio debe controlar (es decir, cómo el custodio deben organizarse y qué recursos deben dedicar a garantizar dicho control). Esto puede derivarse del Considerando 83 MiCA, que aclara que el custodio será responsable de un incidente relacionado con las TIC, incluido un incidente derivado de un ciberataque, robo o cualquier fallo de funcionamiento.

Por lo tanto, la responsabilidad en virtud del art. 75(8) MiCA resulta de un ejercicio de separación entre incidentes imputables y no imputables. A este respecto, cabe señalar que la AEVM interpreta el considerando 83 de la MiCA en el sentido de que los CASP que utilicen infraestructuras de DLT sin permiso que no controlen ni gestionen (es decir, que no exista ningún acuerdo contractual) están exentos de esta responsabilidad. Aunque esto establece claramente un incentivo para subcontratar aplicaciones DLT sin permiso en lugar de las aplicaciones DLT con permiso, la AEVM trata de subsanar esta deficiencia proponiendo obligaciones en caso de que se produzca una perturbación que afecte a una DLT sin permiso, como, por ejemplo, comunicar la perturbación al cliente junto con los riesgos asociados y su propia exclusión de responsabilidad en tales casos y, por último, actuar en el mejor interés de los clientes. Además, los CASP deben seguir siendo responsables de

[80] Art. 75(4) MiCA.

cualquier pérdida relacionada con sus propios contratos inteligentes, como hackeos o exploits, independientemente de si se despliegan en una DLT con o sin permiso.[81]

A primera vista, podría parecer contradictorio, ya que por un lado se habla de una responsabilidad sin culpa, y por otro, se menciona que esta queda excluida si el siniestro no es imputable. Sin embargo, no hay una contradicción real si entendemos el marco de MiCA como un intento de equilibrar ambas cuestiones. La responsabilidad objetiva del custodio (Artículo 75(8)) se activa siempre que el incidente sea imputable al custodio, es decir, que sea algo que debía y podía prever o gestionar (por ejemplo, garantizar la seguridad de sus sistemas frente a ciberataques).Sin embargo, si el evento está fuera de su control razonable, como un caso de fuerza mayor o un ataque imprevisible a pesar de medidas adecuadas, entonces no sería imputable y, por lo tanto, no habría responsabilidad.

Entonces, no se contradicen, sino que están conectadas por la delimitación de lo que significa "imputable". La clave está en la interpretación práctica del control que el custodio debe ejercer sobre sus operaciones y los recursos necesarios para prevenir pérdidas. Esto introduce un grado de flexibilidad, pero también plantea desafíos sobre qué constituye "control razonable", un tema que seguramente generará debates y posibles litigios en su aplicación práctica.

3.6. Evaluación crítica de MiCA

En este epigrafe vamos a medir la solidez de MiCA a la luz de las numerosas deficiencias inherentes a la configuración y conducta del custodio en el contexto del criptoinvierno. Desde esta perspectiva, MiCA se considera un mitigante de la crisis al mejorar la resistencia de los custodios.

Como hemos dicho, MiCA garantiza que el depositario es un fiduciario debidamente autorizado, sólidamente organizado y gobernado, sujeto a requisitos prudenciales buscando el equilibrio de los conflictos de intereses y gestión de riesgos operativos. Los depositarios deberán segregar sus propios activos de los activos de sus clientes y evitar la reutilización de estos últimos por cuenta propia. Las obligaciones de transparencia relativas a las tenencias

[81] Cf. ESMA, *Consultation Paper Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation*" (MiCA) – Segundo documento de consulta, ESMA75-453128700- 438, pp. 19, 21, 22

de los clientes así como el régimen de responsabilidad del depositario persiguen el mismo objetivo. [82]

Sin embargo, incluso cuando las condiciones de autorización y funcionamiento son sólidas, la resistencia global deseada puede no lograrse cuando los proveedores de servicios tienen la capacidad de evitar, o tomar medidas para eludir, las condiciones de autorización y funcionamiento de MiCA.

Vemos aquí tres puntos de entrada a través de los cuales socavar la resistencia institucional: El ámbito de aplicación de la MiCA, las disposiciones sobre responsabilidad y las normas de externalización.

3.6.1. Alcance

La eficacia de cualquier norma de MiCA está limitada por su ámbito de aplicación: lo que queda fuera de las normas no es abordado por ellas de forma eficaz. Argumentamos aquí que las limitaciones a las aplicaciones totalmente descentralizadas, la definición de actividades reguladas como tales y la autocustodia pueden socavar la eficacia de las normas de custodia de la MiCA.

a) ¿Alternativa descentralizada?

MiCA cubre las aplicaciones totalmente descentralizadas sólo en la medida en que se califiquen como "empresa". Si los reguladores interpretan la definición de "empresas" en sentido amplio, esto obligará a muchas aplicaciones descentralizadas a introducir acuerdos de gobernanza tal y como exige el Título V de la MiCA. Se puede argumentar que esto va en contra de la intención de que MiCA se centre únicamente en los cripto servicios centralizados. Desde el punto de vista práctico, los reguladores pueden tener dificultades a la hora de identificar a las personas responsables de la aplicación y de hacer cumplir las órdenes en un entorno ampliamente internacional.[83]

Hemos establecido además que el alcance de las normas de custodia de MiCA en el Art. 3(1)(17) MiCA se basa en una delimitación de los monederos custodiados y no custodiados. La solidez de MiCA aumenta cuando más aplicaciones DeFi entran en el ámbito

[82] Art. 75(8), (6) MiCA

[83] Zetzsche,Arner,Buckley, *Decentralized Finance* (DeFi), pp. 172-203

de aplicación de MiCA, y disminuye cuando más soluciones de monedero permanecen sin regular. Esto resulta aún más relevante, ya que desde el anuncio de la introducción de MiCA y su intención de regular de forma más estricta las soluciones criptográficas centralizadas, se ha observado una creciente inclinación hacia las soluciones sin custodia.[84]

b) Restricciones a las actividades reguladas

Por último, la resiliencia institucional está potencialmente en riesgo debido a la definición de los servicios de criptoactivos. Servicios como el criptopréstamo y la criptofijación quedan potencialmente fuera del ámbito de aplicación, ya que no prestan servicios regulados de criptoactivos (por ejemplo, servicios de custodia o transferencia).[85]

A menudo, los CASP multifunción combinan la custodia con actividades de asunción de riesgos, como la negociación por cuenta propia. Cómo trata MiCA estos servicios además de las normas de conflicto es algo confuso: incluso los "CASP significativos" sujetos a normas a medida en virtud del Título V Capítulo 5 MiCA se clasifican en significativos debido únicamente al número de clientes, sin considerar otros factores de riesgo. La prestación de múltiples servicios como característica de los CASP multifunción ha sido un buen criterio para determinar la complejidad.[86]

En estos casos, la cobertura reglamentaria de los servicios secundarios, como la transferencia y la custodia, dictará la resistencia institucional. Aquí, la primera línea de batalla estará entre la *custodia de* criptoactivos en nombre de los clientes como un servicio auxiliar de criptopréstamo y criptoapuesta, en contraste con la *transferencia* de criptoactivos *a otros* (clientes y no clientes) en interés de los clientes; tenga en cuenta que la transferencia de criptoactivos es una actividad regulada diferente de la custodia, a la que no se aplica el art. 75 MiCA, aunque MiCA contiene pocos detalles sobre lo que implica.[87]

---

[84] Zetzsche, D. A., Buckley, R. P., Arner, D. W., & van Ek, M. (2023), *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*, *Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies*, European Parliament, Luxembourg (2023): 23-27.

[85] Art. 70 y 82 MiCA respectivamente.

[86] Art. 72 MiCA. En el contexto de la gestión de conflictos de intereses, la AEVM propone políticas, procedimientos y prácticas de remuneración de los CASP, cf. ESMA *Consultation Paper on Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation* (MiCA), ESMA74-449133380-425, p. 38.

[87] La MiCA no establece ninguna disposición sustantiva aparte del art. 82 MiCA. Se centra en las definiciones. Véase el art. 3(1)(26) MiCA ("prestar servicios de transferencia de criptoactivos en nombre de clientes" significa

En segundo lugar, cuando la custodia es un elemento, potencialmente inicial, del servicio, inevitablemente se librará una batalla sobre hasta qué punto el consentimiento de los clientes permite un tratamiento diferente del previsto en el art. 75 MiCA. Sin embargo, cuando la reutilización depende del consentimiento del cliente, ¿qué límites implícitos existen con respecto a la reutilización? ¿Hay que ofrecer alguna compensación a los clientes, como condición previa para un consentimiento válido? ¿Cuáles son los requisitos legales para un consentimiento válido a la reutilización?

Las respuestas a estas preguntas determinarán la eficacia con la que MiCA garantiza la resistencia institucional.

c) ¿La responsabilidad como barrera de entrada?

Otra razón que podría socavar la resistencia institucional se deriva de las disposiciones sobre responsabilidad del Art. 75(8) MiCA: cuando los intermediarios serios y bien financiados deben temer la responsabilidad, pueden decidir salirse del mercado. Dado que el mercado criptográfico es pequeño, en términos relativos, mantenerse al margen del cripto es una de las varias opciones que tienen los intermediarios financieros a la hora de decidir su estrategia criptográfica. Si bien es poco probable que a largo plazo se opte por la exclusión total, ya que los intermediarios corren el riesgo de perder oportunidades, una estrategia viable y ya observada consiste en establecer filiales con escasa financiación, dejando el balance principal fuera del ámbito de aplicación de las normas de responsabilidad. En la medida en que la mayoría de los grandes intermediarios se abstengan de cripto, y no estén dispuestos a considerar la existencia de cripto-activos, el mercado de cripto seguirá siendo pequeño, en términos relativos, y la abstención de cripto, en general, *sigue siendo* una opción viable[88].

En este contexto, cabe destacar que la MiCA no exige a los custodios una capitalización similar a la de un banco; por lo tanto, los criptocustodios pueden ser entidades escasamente capitalizadas en virtud de la MiCA. Cuando los custodios sólo aportan el capital mínimo, es previsible que las pérdidas puedan acumularse fácilmente hasta un importe en el

prestar servicios de transferencia, en nombre de una persona física o jurídica, de criptoactivos de una dirección o cuenta de libro mayor distribuido a otra).

[88] Zetzsche, Dirk Andreas; Annunziata, Filippo y Sinnig, Julia, "Digital Assets, MiCA and EU Investment Fund Law" (November 18, 2023). Available at SSRN: https://ssrn.com/abstract=4637019 or http://dx.doi.org/10.2139/ssrn.4637019

que el capital del custodio sea insuficiente para compensar a los clientes por las pérdidas. En este sentido, la responsabilidad es un arma de doble filo. Si bien puede ayudar a los clientes e inversores de criptomonedas, también puede evitar a los intermediarios sólidos, bien gobernados y financiados que los mercados de criptomonedas tanto necesitan. En ausencia de intermediarios bien financiados que puedan compensar a los poseedores de tokens en caso de pérdidas, las normas de responsabilidad son poco beneficiosas en la práctica.[89]

Para demostrar la importancia de nuestro argumento, debemos tener en cuenta el uso que hacen los custodios, y especialmente los proveedores de monederos vinculados a bolsas, del "almacenamiento en caliente" de claves privadas de múltiples clientes. Estas herramientas de almacenamiento están constantemente conectadas a Internet, para garantizar la eficiencia en tiempo y costes. Se ha dicho que estos "monederos calientes" son "un atractivo tarro de miel para los piratas informáticos" y son más vulnerables que los métodos de almacenamiento de claves en frío (fuera de línea). [90]

d) ¿Subcontratación?

Otro factor que podría socavar la resistencia institucional se deriva de las normas de externalización del art. 73 MiCA. Dado que las normas CASP se aplican únicamente a las entidades de la UE, aunque muchos criptointermediarios residen fuera de la UE, la externalización a entidades de fuera de la UE debilita potencialmente la resistencia institucional proporcionada por la MiCA. Esto es especialmente cierto porque la MiCA no aborda suficientemente varias cuestiones relacionadas con la externalización de las funciones de custodia.[91]

Por ejemplo, en TradFi, en los casos de externalización de la función de custodia, se establece que los activos del cliente estarán segregados de los activos propiedad del custodio,

---

[89] El art. 67 MiCA y el Anexo IV MiCA exigen que los depositarios dispongan de un capital reglamentario de 125.000 euros más ¼ de los gastos generales fijos del año anterior. Por ejemplo, si los gastos generales fijos ascienden a 3 millones de euros (que estimamos que es una cantidad razonable para una CASP bastante grande con 20 a 30 empleados), el capital reglamentario total disponible ascenderá a 875.000 euros. En ausencia de negocio bancario adicional, estos custodios difícilmente podrán cubrir grandes pérdidas de los titulares de tokens.

[90] Cf. FMI, *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Asset"* (Policy Paper, septiembre de 2022) https://www.imf.org/en/Publications/fintech- notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked- Crypto-Assets- 523715 [ultimately Consulta: 9/02/2025] ,p. 22.

[91] Art. 2 (1) MiCA

de los activos propiedad del tercero, así como de los activos pertenecientes a otros clientes del tercero. No nos parece que sea el mismo caso en MiCA. Esto no cambia fundamentalmente por el hecho de que la CASP tenga que mantener ciertos registros y almacenar todos los datos de la CASP[92] ni la comunicación con el subcustodio y prever la insolvencia del subcustodio en su plan de continuidad de negocio. Aunque la MiCA exige la segregación de los activos del cliente de los activos propios del custodio, carece de normas específicas sobre la externalización de la criptocustodia similares a las de la legislación de la UE sobre fondos de inversión. [93]

Con respecto a la segregación de activos por parte del subcustodio, la MiCA es ambigua en cuanto a si requiere la segregación en la cadena (es decir, con direcciones de cadena de bloques separadas), o si es suficiente fuera de la cadena (es decir, con un sistema de mantenimiento de registros segregado). Además, MiCA no responde a la pregunta de si el custodio puede confiar en los registros del subcustodio para la obligación de mantenimiento de registros del custodio. Por último, MiCA no prevé salvaguardias para la insolvencia del subcustodio - y por lo tanto no aborda un problema de toda la criptoindustria: el hecho de que un CASP tenga información sobre la cuenta del subcustodio no asegura que los activos estén segregados en caso de insolvencia del subcustodio, ni que el CASP tenga capacidad legal en los procedimientos legales y de insolvencia relacionados con los activos del subcustodio. Dado que este último punto se refiere a la resistencia de los activos, lo abordaremos en ese contexto en la siguiente sección.[94]

---

92 Art. 11(d) GFIA, art. 22 bis, apartado 3, OICVM, Considerando 2, Reglamento Delegado (UE) 2018/1618 de la Comisión, de 12 de julio de 2018, por el que se modifica el Reglamento Delegado (UE) n.º 231/2013 en lo que respecta a las obligaciones de custodia de los depositarios C/2018/4377, DO L 271 de 30 de octubre de 2018, p. 1-5, Art. 2, apartado 1, letra d), Directiva Delegada (UE) 2017/593 de la Comisión.

93 Según la AEVM, el plan de continuidad de la actividad de la CASP tendrá en cuenta el impacto potencial de la insolvencia u otros fallos de terceros proveedores de servicios, el fallecimiento de una persona clave y, en su caso, los riesgos políticos en la jurisdicción del proveedor de servicios. Cf. ESMA *Consultation Paper on Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation* (MiCA), ESMA74-449133380- 425, p.86.

94 Sobre las cuestiones derivadas de esa confianza en relación con los depositarios de fondos de inversión, Riassetto Isabelle, "La ségrégation des instruments financiers et le dépositaire d'OPC", *Revue de Droit Bancaire et Financier*, septiembre de 2018, pp. 25-31.

3.6.2. Resistencia de los activos

Mientras que, a pesar de pequeñas deficiencias, MiCA refuerza claramente la resistencia institucional, estamos menos convencidos de que MiCA proporcione el marco necesario con respecto a la resistencia de los activos (es decir, un marco que garantice la existencia de los activos cuando se produzcan cambios operativos en el libro mayor distribuido (por ejemplo, bifurcaciones, airdrops), cuando el emisor de tokens o la aplicación DeFi experimenten dificultades o, por último, cuando el criptocustodio, o terceras partes como los otros clientes del custodio, estén en quiebra o cerca de la quiebra).

Si bien la MiCA aborda la angustia y el mal funcionamiento del emisor del token sólo en el contexto de las ART y las EMT en sus Títulos III y IV, lo hace al abordar los cambios (por ejemplo, airdrops, bifurcaciones o eventos similares) en el libro mayor distribuido subyacente para todos los tipos de criptoactivos de dos maneras: MiCA prevé la "regla de sustitución "del art. 75(4)[95] y, por lo tanto, la obligación del custodio de facilitar el ejercicio de los derechos de los clientes resultantes de tales acontecimientos, junto con el deber fiduciario del custodio y sus obligaciones de información con respecto al cliente.

Por último, para el caso de que el custodio, subcustodios o terceros se encuentren en dificultades, disfunciones o conductas indebidas que afecten a los criptoactivos de los clientes, los arts. 70 y 75 MiCA *establecen, entre otras cosas*: la obligación del custodio de salvaguardar los activos y derechos de acuerdo con una política de custodia adecuada, especialmente en caso de insolvencia del custodio; la obligación de mantener registros detallados para cada cliente; la obligación de segregar los activos de los clientes de los propios activos del custodio; la prohibición de reutilización de activos por cuenta propia del custodio; y la responsabilidad de este último por pérdidas de activos.

El análisis de la eficacia de la resistencia de los activos requiere (a) cierto contexto en relación con el derecho privado sobre criptoactivos, seguido de (b) un breve examen del potencial de la regulación financiera para garantizar la resistencia de los activos. Sobre esta base, resumimos nuestras preocupaciones sobre la resistencia de los activos tras la adopción de la MiCA.

[95] Cf. Art. 66, 72, 75(2), (7), (5) MiCA

a) Raíces en el proceso legislativo de la UE: Base de Derecho Privado en duda

Debido a la naturaleza de DLT, la existencia del activo depende del reconocimiento por parte de otros nodos y del funcionamiento de estos. En este contexto multipartito, la eficacia de la protección jurídica depende de la naturaleza y el alcance de los derechos que el cliente tiene sobre los criptoactivos mantenidos en custodia, en virtud del Derecho privado aplicable.

Si bien la MiCA exige a los criptocustodios que salvaguarden los derechos de propiedad de sus clientes en caso de insolvencia del custodio con arreglo a la legislación aplicable en materia de insolvencia, la legislación sobre insolvencia en el ámbito de las criptomonedas está muy poco desarrollada en las jurisdicciones de la UE. De hecho, a los custodios les resultará difícil identificar qué medidas deben adoptar realmente para tomar disposiciones en caso de insolvencia propia o de suspensión de las operaciones de las aplicaciones DeFi.[96]

Además, dada la incertidumbre jurídica generalizada en relación con la titularidad y los derechos de propiedad de los activos digitales, será interesante ver cómo los CASP que actúan para clientes de varias jurisdicciones cumplen los requisitos mencionados. En particular, la falta de un marco jurídico armonizado y la ambigüedad general anima a los custodios existentes a establecer en sus términos y condiciones que el cliente sólo tiene un derecho contractual no garantizado sobre los criptoactivos confiados, y/o a establecer acuerdos de transferencia de titularidad.[97]

b) Regulación financiera como atenuante del subdesarrollado Derecho privado

Hasta cierto punto, la regulación de productos para ARTs y EMTs en los Títulos III y IV MiCA sustituye esta laguna del Derecho privado con respecto a las criptomonedas. Los emisores de ARTs y EMTs están sujetos a requisitos de licencia, custodia y prudenciales -

[96] Según la mayoría de las leyes de insolvencia, sólo las personas y las entidades pueden declararse insolventes, y no está claro si las solicitudes de DeFi pueden calificarse como una de las primeras.

[97]Woxholth, Jannik; Zetzsche, Dirk Andreas,M; Buckley, Ross P. y Arner, Douglas W., "Competing Claims to Crypto assets", *Uniform Law Review*, vol. 28, t. 2, 2023. Para un argumento de que la racionalización de las leyes de insolvencia de criptomonedas es una prioridad. Véase. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & van Ek, M. (2023*), Remaining regulatory challenges in digital finance and crypto-assets after MiCA, Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament*, Luxembourg (2023): 23-27.

incluyendo planes de rescate y recuperación - para los emisores de ART y EMT. Además, se exige a los emisores que pongan fin a sus actividades cuando la continuidad de su negocio esté en peligro. De este modo se garantiza la resistencia de los activos incluso allí donde el Derecho privado está en gran medida ausente. Necesariamente, la puesta en marcha y la eficacia operativa de estos planes de enterramiento requieren importantes recursos por parte del emisor y de la agencia de supervisión. Esto explica por qué el Título II MiCA sobre otros criptoactivos se abstiene de normas similares - y por lo tanto porqué los tenedores de tokens de otros activos permanecen en gran medida desprotegidos.[98]

c) Protección de activos en caso de fallos y disfunciones del depositario o de terceros

Por último, si bien la MiCA define los derechos y obligaciones del depositario y de sus clientes en caso de fallo o mal funcionamiento del propio depositario, estas normas ofrecen poca protección de los activos frente a terceros, como los demás clientes del depositario, las contrapartes y los agentes malintencionados.

aa) Custodia y segregación de activos

En cuanto a la protección de los activos en caso de malas prácticas o incumplimientos de los otros clientes del custodio, MiCA solo aclara la obligación de segregar los activos de los clientes de los propios activos del custodio "operativamente" (es decir, en la DLT utilizando direcciones de blockchain separadas) y "legalmente" (es decir, con un sistema segregado de mantenimiento de registros). Esto contrarresta la práctica del custodio de utilizar, por razones de tiempo y coste, direcciones comunes de monederos de blockchain mezclando los activos de múltiples clientes con sus propios activos. Sin embargo, la MiCA no exige la segregación cliente por cliente en la DLT. Esto permite el uso de carteras ómnibus (es decir, direcciones comunes de blockchain en las que se agrupan los criptoactivos de múltiples clientes). En este caso, la protección de los criptoclientes carece de la rigidez de TradFi, donde se permite el uso de monederos ómnibus cuando la custodia se delega y bajo estrictos requisitos de segregación. A su vez, los criptoclientes permanecen expuestos no sólo al elevado riesgo de ciberataques, sino también a los riesgos derivados de la insolvencia de *los demás* clientes del custodio, cuyos activos se agrupan dentro del mismo monedero ómnibus. Obsérvese que los poseedores de tokens no tienen información sobre estos otros clientes y, por lo tanto, no disponen de medios para protegerse retirándose antes de tiempo o emitiendo

[98] Título III Capítulos 2, 3, 6 MiCA.

órdenes judiciales. Esta asimetría de información se suma a las incertidumbres jurídicas relativas a la naturaleza de los derechos de los tenedores de tokens en la cuenta ómnibus de criptomonedas.[99]

En cuanto a la protección de los activos en caso de malas prácticas o fallos de cualquier subcustodio, la MiCA no prevé disposiciones granulares que aborden la obligación de segregación que deberá asumir el subcustodio y la protección de los activos custodiados en caso de insolvencia del subcustodio.

bb) Acuerdos de reutilización y transferencia de títulos

Además, en cuanto a la protección de los activos en caso de malas prácticas o fallos del depositario o de terceros, como las contrapartes del depositario, el art. 70 (1) MiCA prohíbe la reutilización de los activos de los clientes por cuenta propia y el considerando 83 MiCA exige que los activos de los clientes estén libres de cargas. Sin embargo, la prohibición absoluta y la redacción restrictiva de estos dejan margen para elusiones. A la luz de las prácticas comunes que combinan varios tipos de reutilización de activos con la falta de especificaciones sobre la función de un intermediario como custodio, proveedor de liquidez o contraparte, consideramos que las normas de la MiCA carecen de granularidad sobre los requisitos legales para la reutilización de activos. Mientras tanto, TradFi establece un nivel adecuado de protección deseable, siendo una de las principales salvaguardias que los acuerdos de transferencia de titularidad sólo se permitan cuando el custodio revele *ex ante* toda la información y los riesgos pertinentes al cliente y obtenga su consentimiento expreso previo[100]

cc) *Control de supervisión y representación frente a terceros*

Por último, el custodio no tiene el mandato de representar los intereses de sus clientes frente a terceros (por ejemplo, supervisando o controlando la conducta de otros CASP), ni tiene

---

[99] Sobre los requisitos de transparencia de las cuentas ómnibus, véase la Recomendación 14, OICV, *Final Report, Policy Recommendations for Crypto and Digital Asset Markets* (Policy Paper 2023) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf,[Consulta 9/02/2025].

[100] Ex. Art. 16(8)-(10) MiFID, Art. 5,6 Directiva Delegada de la Comisión (UE) 2017/593.Sobre los acuerdos de transferencia de titularidad en relación con los criptoactivos, véase además OICV, *Final Report, Policy Recommendations for Crypto and Digital Asset Markets* (Policy Paper, 16 de noviembre de 2023) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf, [ultimately consulta 9/02/2025]; FBS, *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final report* (Policy Paper, 17 de julio de 2023) https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/. [ultimately consulta 9/02/2025].

capacidad legal expresa para representar a los clientes y sus intereses en procedimientos judiciales frente a terceros en virtud de la MiCA. Aunque el mandato de representar a los clientes podría derivarse del deber fiduciario del custodio, sin legitimación cualquier acción legal está cargada de riesgos.

Aunque se podría argumentar que la legitimación se derivaría del registro del depositario en nombre de sus clientes en el libro mayor distribuido, esto estaría en contradicción con los modelos de verdadera segregación en el libro mayor e incluso cuando se da la legitimación, la incertidumbre en el criptoderecho privado hace que sea arriesgado emprender acciones legales en nombre de los clientes.[101] En este caso, MiCA carece de la claridad y sencillez de la regulación TradFi: los depositarios de fondos de inversión sí representan los intereses de sus clientes ejerciendo la supervisión, y también tienen, en la mayoría de las legislaciones, legitimación en procedimientos como competencia accesoria a la custodia, donde las reclamaciones contra el gestor de fondos. Dado que las disposiciones de la regulación financiera sobre fondos de inversión han sustituido durante mucho tiempo a las incertidumbres que rodean al derecho privado de los organismos de inversión colectiva en un contexto transfronterizo, la regulación del depositario TradFi proporciona un modelo útil para la criptocustodia, que la MiCA no implementó. [102]

[101] Por ejemplo, cuando los activos de cada cliente tienen su propia cartera de blockchain dirección

[102] Art. 22 (3)-(4) UCITSD y 21 (7), (9) AIFMD.

CONCLUSIÓN.

A lo largo de este trabajo, ha quedado de manifiesto cómo el avance tecnológico no solo transforma los mercados y las dinámicas económicas, sino que también plantea un desafío constante para los reguladores. La rapidez con la que surgen nuevas innovaciones tecnológicas, especialmente en el ámbito de los criptoactivos y las finanzas descentralizadas, contrasta con el ritmo mucho más lento y deliberado del proceso legislativo. Esto genera un desfase natural entre la realidad del mercado y las herramientas normativas disponibles, obligando al legislador a adaptarse continuamente a necesidades y riesgos emergentes.

Como se ha introducido en el capítulo 1, las dificultades del legislador para regular este ámbito son evidentes, tanto por la complejidad técnica como por la naturaleza cambiante y descentralizada de los criptoactivos. Incluso contando con MiFID de precedente en la regulación de los mercados financieros, el marco normativo no ha logrado anticiparse por completo a los desafíos de la economía digital. MiCA, aunque ambicioso en su alcance, no está exento de lagunas y zonas grises, evidenciando que la ley llega, casi siempre, en un esfuerzo por alcanzar una realidad que ya le lleva ventaja.

En este contexto, queda claro que la regulación deberá mantener un carácter flexible y dinámico, capaz de ajustarse a un entorno tecnológico en constante cambio. Sin embargo, este proceso no estará exento de tensiones entre la necesidad de proporcionar seguridad jurídica y la presión por mantener un espacio adecuado para la innovación. Un ejemplo de esta dificultad se observa en los problemas de interpretación jurídica relacionados con el ámbito de aplicación de MiFID y MiCA, especialmente en la definición de "instrumento financiero". Mientras que MiFID establece criterios específicos para determinar qué activos entran dentro de su regulación, la ambigüedad en la clasificación de ciertos criptoactivos ha generado incertidumbre sobre su tratamiento normativo. MiCA, por su parte, intenta cubrir este vacío regulatorio, pero su delimitación con respecto a MiFID sigue siendo un área de debate, particularmente en lo que respecta a los tokens con características híbridas. Por tanto, el reto del legislador no solo será reducir este desfase, sino también garantizar que las futuras normativas sean lo suficientemente resilientes para afrontar la complejidad de las tecnologías por venir, ofreciendo claridad interpretativa sin frenar la evolución del sector.

En el segundo capítulo se muestra la importancia crítica de los custodios de criptoactivos dentro del ecosistema de las finanzas digitales. Estos actores, encargados de

salvaguardar los activos digitales de sus clientes, desempeñan un papel central para garantizar la seguridad y la confianza en los mercados de criptoactivos. Sin embargo, también se ha manifestado que este ámbito presenta importantes deficiencias regulatorias y operativas que lo convierten en un punto de vulnerabilidad.

Los numerosos casos de fraude y fallos a gran escala, como los escándalos que han sacudido al sector en los últimos años, demuestran que la falta de controles adecuados y de una supervisión efectiva puede tener consecuencias devastadoras. Ejemplos como el colapso de FTX o la pérdida de fondos de clientes debido a ciberataques subrayan las limitaciones de los marcos normativos actuales y la necesidad urgente de establecer estándares claros y exigentes para los custodios. Estas situaciones no solo afectan a los titulares de criptoactivos, sino que erosionan la confianza en el sector y dificultan su desarrollo sostenible.

En respuesta a estas deficiencias, las propuestas internacionales para regular a los custodios de criptoactivos están adquiriendo un protagonismo cada vez mayor. Iniciativas como MiCA en la Unión Europea y, recomendaciones políticas del FSB, el FMI y la IOSCO aunque ambiciosas, son solo un paso inicial en la construcción de un marco que proteja adecuadamente los intereses de los usuarios. Estas propuestas buscan abordar cuestiones clave como la responsabilidad legal en caso de pérdidas, la segregación de activos y la prevención de prácticas abusivas por parte de los custodios. Sin embargo, como se ha analizado, su implementación aún plantea desafíos importantes, especialmente en un entorno global donde las regulaciones no siempre son coherentes entre jurisdicciones.

Por último, el tercer capítulo ha desarrollado un análisis exhaustivo de la propuesta europea de regulación de criptoactivos contenida en el Reglamento MiCA, con un enfoque especial en las reglas de custodia, la naturaleza descentralizada de ciertos activos digitales y las obligaciones específicas para los proveedores de servicios. También se ha evaluado la interacción de estas normas con otros marcos regulatorios como MiFID, ofreciendo una perspectiva jurídica y analítica sobre los avances y limitaciones del reglamento.

En primer lugar, MiCA representa un esfuerzo significativo por parte del legislador europeo para estructurar un marco regulatorio europeo que responda a las particularidades del ecosistema de criptoactivos adaptándose paulatinamente a los 27 estados miembros con sus diferentes culturas, idiomas, tradiciones... La custodia de criptoactivos, como elemento

central del análisis, adquiere especial relevancia en este contexto. MiCA introduce reglas diseñadas para garantizar la protección de los activos de los usuarios frente a riesgos de fraude, pérdida o insolvencia de los custodios. Esto supone un cambio importante frente a prácticas comunes en la industria, donde históricamente los custodios han limitado su responsabilidad legal, dejando a los titulares de los activos con poca o ninguna protección. En este sentido, el Artículo 75(8) de MiCA establece la responsabilidad del custodio por la pérdida de activos, lo que marca un punto de inflexión en la manera en que se regulan estas actividades.

No obstante, el capítulo también ha abordado las dificultades inherentes a la regulación de la custodia en un ecosistema tan diversificado. La naturaleza descentralizada de ciertos criptoactivos plantea desafíos para el concepto tradicional de custodia, especialmente cuando no existe un responsable identificable o cuando el control de los activos depende exclusivamente de las claves criptográficas. MiCA intenta resolver esta ambigüedad al definir el control sobre las claves como un criterio esencial de "custodia". Sin embargo, el surgimiento de soluciones alternativas, como las custodias híbridas o intermedias, y las aplicaciones DeFi totalmente descentralizadas, desborda parcialmente el alcance de la regulación, lo que pone de manifiesto la necesidad de ajustar las normas conforme evoluciona el mercado.

Por otro lado, se ha examinado cómo MiCA regula los proveedores de servicios de criptoactivos (CASPs), imponiendo requisitos estrictos en términos de autorización, transparencia y gestión de riesgos. Este enfoque es un intento de reforzar la confianza en el sector, limitando los abusos que han caracterizado a algunos actores en el pasado. Sin embargo, el marco de MiCA presenta ciertas lagunas, especialmente cuando se compara con MiFID, que regula de manera más robusta y precisa los servicios financieros tradicionales. Mientras que MiFID cuenta con décadas de desarrollo normativo y experiencia en su implementación, MiCA aún se enfrenta al desafío de establecer un marco igualmente sólido en un sector que evoluciona a una velocidad mucho mayor.

Además, MiCA introduce un enfoque innovador al reconocer y abordar las particularidades de los criptoactivos descentralizados, pero lo hace bajo una perspectiva que no siempre encaja con las realidades prácticas del sector. Por ejemplo, la dificultad de supervisar entidades o aplicaciones descentralizadas plantea dudas sobre cómo garantizar la

protección efectiva del consumidor en estos entornos. El Considerando 83 de MiCA, que establece la responsabilidad de los custodios por incidentes relacionados con las TIC, como ciberataques o fallos técnicos, refleja este esfuerzo por ampliar las obligaciones de los custodios, pero también subraya la necesidad de definir claramente los límites de su responsabilidad.

En comparación con MiFID, MiCA refleja un intento de adaptar principios regulatorios tradicionales a un mercado emergente. Sin embargo, como se ha evidenciado, el avance tecnológico y la innovación en el sector de los criptoactivos tienden a superar la capacidad del regulador para anticiparse a las necesidades del mercado. Este desfase normativo plantea interrogantes sobre la capacidad de MiCA para mantenerse relevante a largo plazo, especialmente frente a soluciones descentralizadas que desafían los conceptos tradicionales de responsabilidad y control.

En conclusión, MiCA representa un primer paso importante hacia la regulación del ecosistema de criptoactivos en la Unión Europea. Si bien aborda muchas de las deficiencias existentes y busca garantizar una mayor seguridad y confianza en el sector, su efectividad dependerá de su capacidad para adaptarse rápidamente a la evolución tecnológica y a las nuevas dinámicas del mercado. El reglamento, aunque ambicioso, deberá ser complementado con ajustes normativos continuos que permitan abordar los retos emergentes, manteniendo un equilibrio entre el fomento de la innovación y la protección de los derechos de los usuarios. Este capítulo evidencia que el éxito de MiCA radica no solo en su diseño actual, sino en la flexibilidad y agilidad del legislador para responder a los desafíos futuros.

CITAS BIBLIOGRÁFICAS

BIBLIOGRAÍA.

Arner,Zetzsche,Buckley,Kirkwood, "The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-202", Universidad de Hong Kong, 2023. [ultimately consulta 9/02/2025].

Andreas ,M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain", 2nd ed., *O'Reilly Media ,*2017.[ultimately consulta: 9/02/2025

Bains, Parma; Ismail, Arif; Melo, Fabiana; y Sugimoto, Nobuyasu, "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets", *IMF Fintech Note*, International Monetary Fund, Washington, septiembre de 2022, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Eliott, B., ... & Zhang, B. Z. (2019). *Global Cryptoasset Regulatory Landscape Study*. Cambridge Centre for Alternative Finance, Faculty of Law, Research Paper, nº23.

Burroughes, Tom (2022), "FTX Collapse May Prompt Big Regulatory Crackdown – Lawyer", *Wealth Briefing Asia,* (Nov. 18, 2022), https://www.wealthbriefingasia.com/article.php?id=196248. [ultima consulta 09.02.2025]

Buterin,V, "Why we need wide adoption of social recovery wallets",2021 https://vitalik.ca/general/2021/01/11/recovery.html [ultimately consulta 9/02/2025].

De Filippi, Primavera and Wright, Aaron, *Blockchain and the Law: the Rule of Code*, Harvard University Press, Harvard, 2018.

Fantato, Damian (2022), "Crypto and Digital Assets Summit", *Financial Times Events* (Nov. 28, 2022), págs… disponible en https://www.ftadviser.com/events-awards/2022/11/28/crypto-digital-assets-summit.

Ferrarini, G. and Giudici, P., "Digital Offerings and Mandatory Disclosure: A Market-Based Critique of MiCA", *European Corporate Governance Institute – Law Working Paper* No. 605/2021); Available at :https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3914768 [ultimately consulta 09.02.2025].

Gareth Jenkinson, "CoinEx hack: Compromised private keys led to$70M theft" *Cointelegraph*, 2023 https://cointelegraph.com/news/coinex-compromised-private-keys-behind-70-million-hack. [ultimately 9/02/2025].

Goforth,C, Guseva,Y, "Regulation of Cryptoassets, American Casebook Series*"*, 2nd ed., *West Academic Publishing,* 2022, pp. 760-781,790.

Inverbots Español. "*La Historia del dinero- El Trueque, Acuñación, Banca y Criptomonedas"*. 21 de Noviembre 2020. https://www.youtube.com/watch?v=-bh3Tt_ZvXQ [ultima consulta 9/02/2025].

Johnson, Leighton, *Security Controls Evaluation, Testing, and Assessment Handbook*, 2ª ed., Academic Press, Oxford, 2020, pp. 524-526.

Kaal,W,Howe,H, "Custody of digital assets", *Jurimetrics*, 2023, vol.63, 2, pp. 169-195.

Lamothe Fernández, Prosper y Lamothe López, Prosper, "¿Cómo valorar los denominados criptoactivos?", *Cuadernos de Información Económica*, nº 277, 2020, pp. 71-80.

Legal Nodes (2023), "The EU Markets in Crypto-Assets (MiCA) Regulation Explained", [en línea], *Legal Nodes*, https://legalnodes.com/article/mica-regulation-explained [ultima consulta 09.02.2025].

Madrid Parra, Agustín (coord.). et al, *Guía de criptoactivos MiCA*, Aranzadi, Pamplona, 2021.

Maia, Guilherme; Vieira dos Santos, João, "MiCA and DeFi "('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance')", *Revista Electrónica de Direito. RED*, vol. 28, nº. 2, 2022, pp. 57-82.

McCarthy, J. (2021), "Evaluating the EU's Digital Finance Strategy: Ambitious Glimpses of Future Regulation?", *Journal of International Banking Law and Regulation*, 36(9), p. 379.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponible online URL: https://bitcoin. org/bitcoin. pdf, 2008, vol. 4, no 2, p. 15. [ultima consulta 09.02.2025]

Noble, E., "Crypto- Assets – Overcoming Impediments to Scaling" (2020); disponible online en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748343. [ultima consulta 09.02.2025]

Riassetto, Isabelle, "La ségrégation des instruments financiers et le dépositaire d'OPC", *Revue de Droit Bancaire et Financier*, nº 5, septiembre de 2018, pp. 25-31.

Saifedean.,A. "El patrón Bitcoin", Universidad de Deusto, Bilbao, 2022. Cap.1 "*Dinero*", pp. 23-33.

Schär, F. (2021). "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets", *Federal Reserve Bank of St. Louis Review*, Vol. 103, No. 2, pp. 153-174.

Siddhartha,Shukla, "Crypto Exchange HTX Hit by $258 Million Outflow After Hack",*Bloomberg*,2023 https://www.bloomberg.com/news/articles/2023-12-10.

Woxholth, Jannik; Zetzsche, Dirk Andreas,M; Buckley, Ross P. y Arner, Douglas W., Competing Claims to Cryptoassets, "Competing Claims to Crypto assets", *Uniform Law Review*, vol. 28, t. 2, 2023, pp. 226–246.

Zetzsche,Arner,Buckley, *Decentralized Finance* (DeFi), pp. 172-203.

Zetzsche, D., Annunziata, F., Arner, D. and Buckley, R., "The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy" (2021), *Capital Markets Law Journal*, 16(2) pp. 203.

Zetzsche, Dirk Andreas; Annunziata, Filippo y Sinnig, Julia, "Digital Assets, MiCA and EU Investment Fund Law" (November 18, 2023). Available at SSRN: https://ssrn.com/abstract=4637019 or http://dx.doi.org/10.2139/ssrn.4637019

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & van Ek, M. (2023), *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*, *Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies*, European Parliament, Luxembourg (2023): 23-27.

Zetzsche, Dirk Andreas and Nikolakopoulou, Areti (2024), "Crypto Custody and Crypto Wallets – An Empirical Assessment" – (March 22, 2024), disponible online en *SSRN*: https://ssrn.com/abstract=4769396 or http://dx.doi.org/10.2139/ssrn.4769396. [ultima consulta 09.02.2025]

Zetzsche, Dirk, Andreas and Sinnig, Julia (2024), "The EU Approach to Regulating Digital Currencies" (January 26, 2024). *Law and Contemporary Problems*, Vol. 87, No. 2, Available at SSRN: https://ssrn.com/abstract=4707830 or http://dx.doi.org/10.2139/ssrn.4707830.

Zetzsche,Woxholth, *EU Regulation of Crypto-assets*(de próxima publicación), Cap. 7. [ultimately Consulta : 9/02/2025]

DOCUMENTOS OFICIALES.

Cf. ESMA, *Consultation Paper Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation*" (MiCA) – Segundo documento de consulta, ESMA75-453128700-438, pp. 19, 21, 22.

Cf. FMI, *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Asset"* (Policy Paper, septiembre de 2022) https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets- 523715 [ultimately Consulta: 9/02/2025] ,p. 22.

Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité Europeo de las Regiones; Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador*, Bruselas, 8.3.2018 COM (2018) 109 final, págs. 1-20.

Documento de consulta publicado el día 29 de enero de 2024 en https://www.esma.europa.eu/sites/default/files/2024-07/ESA_2024_12_Consultation_Paper_Art_97_MiCA_Guidelines.pdf.

EBA, *Report on the Use of Digital Platforms in the EU Banking and Payments Sector (EBA/REP/2021/26* (September 2021).

FMI, *Elements of Effective Policies for Crypto Assets* (Policy Paper, febrero de 2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements- of-Effective-Policies-for-Crypto-Assets-530092, [ultimately 9/02/2025/ (denominado en el cuadro 1 "FMI (2023)"); FMI, "*Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets"* (Política) (Policy Paper, septiembre 2022).

FSB, *Global Regulatory Framework for Crypto-Asset Activities* (Policy Paper, 17 de julio de 2023), https://www.fsb.org/wp-content/uploads/P170723-1.pdf, [ultimately consulta :9/02/2025]; FSB, *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final report* (Policy Paper, 17 de julio de 2023), https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-. supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/. [ultimately consulta 9/02/2025] (denominado en el cuadro 1 "FSB (2023)").

IOSCO, *Informe final, Recomendaciones políticas para los mercados de criptomonedas y activos digitales*. Documento Política,16 noviembre 2023) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf [ultimately consulta 9/02/2025]

OICV, *Final Report, Policy Recommendations for Crypto and Digital Asset Markets* .Policy Paper 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf,[Consulta 9/02/2025].

Propuesta inicial de la Autoridad Europea de Valores y Mercados (AEVM), también deberán llevar registros detallados de los acuerdos de externalización y de los servicios y actividades externalizados. Cf. Documento de consulta de ESMA sobre estándares técnicos que especifican ciertos requisitos del Reglamento sobre Mercados de Criptoactivos (MiCA) - segundo documento de consulta, ESMA75-453128700-438, pp. 162, 171-172.

Propuesta inicial de la AEVM, las DLT sin permiso se considerarán una forma de recurso de "bien común", mientras que el uso de una DLT con permiso operada por una empresa comercial probablemente se basará en contratos disponibles para productos de blockchain de "marca blanca"; en cuyo caso puede considerarse como un "proveedor tercero". Cf. ESMA Consultation Paper on Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper, ESMA75-453128700-438, p. 19. Esta calificación fomenta la externalización a aplicaciones que el proveedor no puede controlar ni supervisar, en particular si se considera junto con los privilegios que la AEVM prevé en materia de responsabilidad en estos casos.

20 SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao (Comunicado de prensa, 5 de junio de 2023) https://www.sec.gov/news/press-release/2023-101 [Consulta: 9/02/2025].

LEGISLACIÓN.

Cf. GFIA, art 11(d); OICVM, art 22a (3); Reglamento Delegado (UE) 2018/1618 de la Comisión, art 2(1)(d).

Considerando 2, Reglamento Delegado (UE) 2018/1618 de la Comisión, de 12 de julio de 2018, por el que se modifica el Reglamento Delegado (UE) n.º 231/2013 en lo que respecta a las obligaciones de custodia de los depositarios C/2018/4377, DO L 271 de 30 de octubre de 2018, p. 1-5, Art. 2, apartado 1, letra d), Directiva Delegada (UE) 2017/593 de la Comisión.

Directiva Delegada de la Comisión (UE) 2017/593.Sobre los acuerdos de transferencia de titularidad en relación con los criptoactivos.

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 (GFIA) [2011], DO L 174/1, art. 21 (8).

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, DOUE de 12.06.2014, página L173/349 y ss.

Directiva Delegada de la Comisión (UE) 2017/593. Sobre los acuerdos de transferencia de titularidad en relación con los criptoactivos.

Directiva 2006/73/CE de la Comisión, de 10 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2004/39/CE del Parlamento Europeo y del Consejo.

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, COM/2020/593 final, disponible online en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020PC0593.

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. o 1093/2010 y (UE) n. o 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, de aquí en adelante Reglamento MiCA.