Alastria Legal

Nº 02 - NOVIEMBRE 2020

EL RÉGIMEN JURÍDICO DE LOS CRIPTOACTIVOS EN LA UE: ESTADO ACTUAL

Blanca Escribano. Jose María Chozas.

THE IRREVERSIBILITY OF HASH AND ITS IMPLICATIONS FOR PRIVACY

Sara Esclapés. Iñigo García de la Mata. Oscar Delgado.

CON LA
COLABORACIÓN DE:

castroalonso

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

EY

Grant Thornton

URÍA
MENÉNDEZ

Editorial
La ruta europea de Alastria

El escenario de incertidumbre en el que estamos inmersos continúa, pero en Alastria seguimos buscando nuestra mejor versión y trabajamos agudizando ingenio, creatividad e innovación. Nuestro foco sigue puesto en reforzar el ecosistema blockchain y nuestros vínculos con la Unión Europea para continuar siendo punta de lanza en la búsqueda de los estándares, las guías y las buenas prácticas en el uso de las tecnologías descentralizadas, teniendo la certeza de que esta tecnología es esencial y debe jugar un papel protagonista en la gestión de la pandemia y en el escenario posterior.

Desde su nacimiento Alastria ha orientado esfuerzos a la generalización y el uso compliant de la tecnología blockchain no sólo en España sino especialmente en Europa. Bajo esta premisa, nuestra asociación ha estado vinculada a las iniciativas del European Blockchain Partnership (EBP), en particular en la European Blockchain Services Infrastructure (EBSI), donde colaboramos de forma muy cercana con la Secretaría General de Administración Digital española para la construcción de la red de blockchain europea, que actualmente cuenta ya con más de 30 nodos y está pendiente el anuncio de la compra precomercial en la que Alastria espera poder participar de la mano de los socios.

También seguimos trabajando en el marco del European Self-Sovereign Identity Framework (ESSIF) para la creación de la identidad digital europea con Alastria ID como referente; en ETSI, el organismo de normalización europeo, liderando la redacción del documento europeo para el rastreo de contactos (para Covid19); en INATBA participamos en sus diferentes workings groups para el diálogo sobre temas de actualidad alrededor de la tecnología; y hemos tenido una participación muy activa en las consultas europeas sobre servicios digitales, regulación de criptoactivos, privacidad y gobernanza de redes, lo que es una muestra de la capacidad de influencia en los foros internacionales.

El debate de todos estos temas que hoy ocupan la agenda internacional sobre blockchain han sido abordados desde hace tiempo en las diferentes comisiones de Alastria, particularmente en el Comité Legal. Somos, en ese sentido, unos adelantados, unos innovadores. Llevamos mucho camino recorrido construyendo futuro y nuestra capacidad de influir en la construcción de esta Europa digital está resultando clave. La segunda edición de la revista es un reflejo de ello, tecnología y derecho en modo coopetición, al más puro estilo Alastria.

Muchas gracias a todos los que habéis participado en esta segunda edición. Continuad con vuestro gran trabajo y mucho ánimo a todos.
Un abrazo fuerte.

Cristina Martínez Laburta
Chief Legal Officer

Publisher

The European Route of Alastria

The scenario of uncertainty in which we are immersed still goes on, but in Alastria we continue searching for our best version and working to sharpen our ingenuity, creativity, and innovation. Our focus continues to be on strengthening the blockchain ecosystem and our links with the European Union, in order to continue to be at the forefront of the search for standards, guidelines and good practice in the use of decentralized technologies, in the knowledge that this technology is essential and must play a leading role in the management of the pandemic and the subsequent scenario.

Since its creation, Alastria has focused its efforts on the generalization and compliant use of blockchain technology not only in Spain, but especially in Europe. Under this premise, our association has been linked to the initiatives of the European Blockchain Partnership (EBP), in particular in the European Blockchain Services Infrastructure (EBSI), where we collaborate closely with the Spanish General Secretariat of Digital Administration for the construction of the European blockchain network, which currently has more than 30 nodes and is pending the announcement of the pre-commercial purchase in which Alastria hopes to participate hand in hand with the partners.

We also continue working within the European Self-Sovereign Identity Framework (ESSIF) for the creation of the European digital identity with Alastria ID as a reference; in ETSI, the European standardization body, leading the drafting of the European document for contact tracing (for Covid19); at INATBA, we participate in its different workings groups for dialogue on current technology issues; and we have taken a very active part in European consultations on digital services, crypto active regulation, privacy and network governance, which is a sign of our capacity to influence international forums.

The debate on all these issues that are currently on the international agenda on blockchain have been addressed for some time in the different Alastria committees', particularly in the Legal Committee. We are, in this sense, advanced and innovative. We have come a long way in building the future and our ability to influence the construction of this digital Europe is proving to be key. The second edition of the magazine is a reflection of this, technology and law in coopetition mode, in the purest Alastria style.

Thank you very much to all who have participated in this second edition.
Please keep it up the good work and stay safe.

Cristina Martínez Laburta
Chief Legal Officer

Alastria Legal

CONSEJO ACADÉMICO
Carmen Alonso Ledesma
Moisés Barrio Andrés
José Luis de Castro Martín
Marta García Mandalóniz
Javier W. Ibáñez Jiménez (presidente)
Ana Felicitas Muñoz Pérez
Jesús Sieira Gil
Alberto Tapia Hermida
Fernando Zunzunegui Pastor

DIRECCIÓN EDITORIAL
Cristina Martínez Laburta
Salvatore Moccia

COMITÉ EDITORIAL
Vicente José García Gil
Luis Garvía Vega
Suzana Maranhão Moreno
Almudena de la Mata Muñoz

EDITA
Asociación Consorcio
Red Alastria, con CIF G 87936159
y domicilio en Alberto Aguilera, 23
28015 Madrid

DISEÑO Y MAQUETACIÓN
Tech Valley S.L
info@dtechvalley.com

legal@alastria.io
@Alastria_
alastria.io

Sumario

Sumary

El régimen jurídico de **los criptoactivos en la UE:** estado actual

Blanca Escribano. José María Chozas.
Abogados. EY

1. INTRODUCCIÓN:

El rápido desarrollo de las tecnologías de registro distribuido (distributed ledger technology o "DLT", por sus siglas en inglés) en los últimos años y su cada vez más extensa adopción en todo el mundo ha venido acompañado del escrutinio de reguladores, a la búsqueda de aprovechar el potencial de la tecnología, pero también de identificar y prevenir riesgos no deseados.

Las instituciones políticas de la Unión Europea ("UE"), encabezadas por la Comisión Europea ("CE"), han estado estudiando el fenómeno durante algún tiempo y desde la aparición de Bitcoin se han planteado diversas iniciativas públicas a nivel europeo. El Plan de Acción de Fintech en 2018[1] allanó el terreno para la publicación de importantes trabajos evaluando la aplicabilidad e idoneidad del marco normativo de servicios financieros de la UE a los criptoactivos[2]. En enero de 2019, la Autoridad Europea de Valores y Mer-

[1] Comisión Europea. (2018), Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic And Social Committee and the Committee of the Regions. FinTech Action plan: For a more competitive and innovative European financial sector. Accedido desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109

[2] Criptoactivo según la Propuesta de Reglamento MiCA, artículo 3.1.b), significa "una representación digital de valor o derechos, que puede transferirse y almacenarse electrónicamente, utilizando un registro distribuido o tecnología similar".

cados ("AEVM") y la Autoridad Bancaria Europea ("ABE"), publicaron sendos informes dirigidos a la CE – el asesoramiento de la AEVM sobre ICOs y criptoactivos ("Informe de la AEVM")[3] y el informe de la ABE sobre criptoactivos ("Informe de la ABE")[4] – destacando una serie de preocupaciones regulatorias. En particular, en los informes se señalaba que la mayoría de criptoactivos se encuentran actualmente fuera del marco normativo sobre servicios financieros de la UE, por lo que no están sujetos a las disposiciones sobre protección de los consumidores e inversores ni sobre integridad del mercado. Por otro lado, cuando los criptoactivos sí entran en el ámbito de la legislación financiera de la UE, su aplicación no siempre es clara e incluso algunas disposiciones pueden obstaculizar el uso de la tecnología DLT. Otro hecho digno de mención es que varios estados miembros de la UE han estado legislando algunos aspectos sobre criptoactivos en áreas no armonizadas a nivel de la UE.

En este contexto, la CE inició una consulta pública sobre el "marco regulador de la UE para los criptoactivos" ("Consulta de la CE")[5], completada del 19 de diciembre de 2019 al 19 de marzo de 2020, en la que se destacó la necesidad de alcanzar "un enfoque común con los estados miembros en materia de criptoactivos para asegurar que [los estados miembros] comprendan cómo aprovechar al máximo las oportunidades que crean y hacer frente a los nuevos riesgos que puedan plantear"[6]. La Consulta de la CE fue seguida de un webinar el 13 de mayo de 2020 que mostró la intención de la CE de regular, al menos en cierta medida, la intersección entre el espacio de los criptoactivos y el financiero, a pesar de la oposición frontal de varios participantes. Tras una revisión extensa de los comentarios y observaciones de la industria y de autoridades reguladoras europeas, la CE publicó en mayo de 2020 un "Documento de trabajo no oficial (non-paper)[7] sobre las propuestas legislativas relativas al marco regulador de la UE para los criptoactivos"[8], actualizado posteriormente en julio de 2020[9].

Como resultado, en septiembre de 2020 la CE publicó la propuesta de reglamento sobre mercados de criptoactivos ("Propuesta de Reglamento MiCA", por su abreviatura en inglés)[10] y la propuesta de reglamento sobre un régimen piloto para infraestructuras de mercado basadas

---

[3] Autoridad Europea de Valores y Mercados. (2019), Advice Initial Coin Offerings and Crypto-Assets. Accedido desde: https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection.

[4] Autoridad Bancaria Europea. (2019), Report with advice for the European Commission on crypto-assets. Accedido desde: https://eba.europa.eu/eba-reports-on-crypto-assets.

[5] Comisión Europea. (2019), Consultation Document on an EU framework for markets in crypto-assets. Accedido desde: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf.

[6] Carta de intenciones de la presidenta electa Von der Leyen al vicepresidente Dombrovskis, 10 de septiembre de 2019.

[7] Un documento de trabajo no oficial ("non-paper") sirve para estimular el debate sobre un asunto particular sin representar la posición oficial de la institución que lo firma.

[8] Comisión Europea. (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Accedido desde: https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf.

[9] Comisión Europea. (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Accedido desde: https://drive.google.com/file/d/1Z-Bl_YSUcKblJCrsOtoQk66z4jtd7Dvkj/view.

[10] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre criptoactivos. Accedido desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN.

en tecnologías de registro distribuido ("Propuesta de Régimen Piloto")[11].

Este trabajo tiene por objeto presentar el marco conceptual con arreglo al cual la CE ha abordado la elaboración de una legislación paneuropea sobre criptoactivos y las medidas que la CE ha propuesto y que aún podría proponer para desarrollar este marco armonizado. Esto nos llevará a través de las siguientes secciones:

· **Una clasificación europea para criptoactivos.** En la primera sección se examinará la clasificación de criptoactivos presentada por la Consulta de la CE, basada en la distinción entre criptoactivos regulados y no regulados, a la luz de las categorías de criptoactivos definidas en la Propuesta de Reglamento MiCA y en la Propuesta de Régimen Piloto.

· **Criptoactivos regulados:** modificaciones en el marco jurídico financiero de la UE para su aplicación efectiva sobre criptoactivos. La segunda sección aborda algunas de las razones señaladas por la CE que justificarían la realización de ajustes en la legislación financiera existente para que pueda aplicarse eficazmente en el campo de los criptoactivos y presenta las posibles medidas legislativas y no legislativas que la CE ha puesto y podría poner en marcha para resolver los problemas identificados durante la Consulta de la CE.

· **Criptoactivos no regulados: un régimen jurídico a medida.** En la tercera sección se examina brevemente cómo el desarrollo de normativa armonizada en la UE podría resolver algunos problemas en el ámbito de los criptoactivos no regulados y se presentan brevemente las líneas principales de la Propuesta de Reglamento MiCA.

II. UNA CLASIFICACIÓN EUROPEA PARA CRIPTOACTIVOS

La Consulta de la CE hace suya la conocida categorización de la Autoridad Suiza de Supervisión de los Mercados Financieros ("FINMA")[12], en la que los criptoactivos se dividen en tres categorías principales, basadas en su función económica: "tokens de pago" ("payment tokens") que pueden servir como medio de intercambio o pago de un producto o servicio, "tokens de inversión" ("investment/asset token") que pueden llevar aparejados derechos de participación en beneficios y "tokens de utilidad" ("utility tokens") que pueden permitir el acceso a o utilización de un producto o servicio específico. Una cuarta categoría sería la de los "tokens híbridos", reservada a los criptoactivos que sirven a más de uno de los fines económicos anteriores simultáneamente o que pueden ver sus características alteradas durante el ciclo de vida del token.

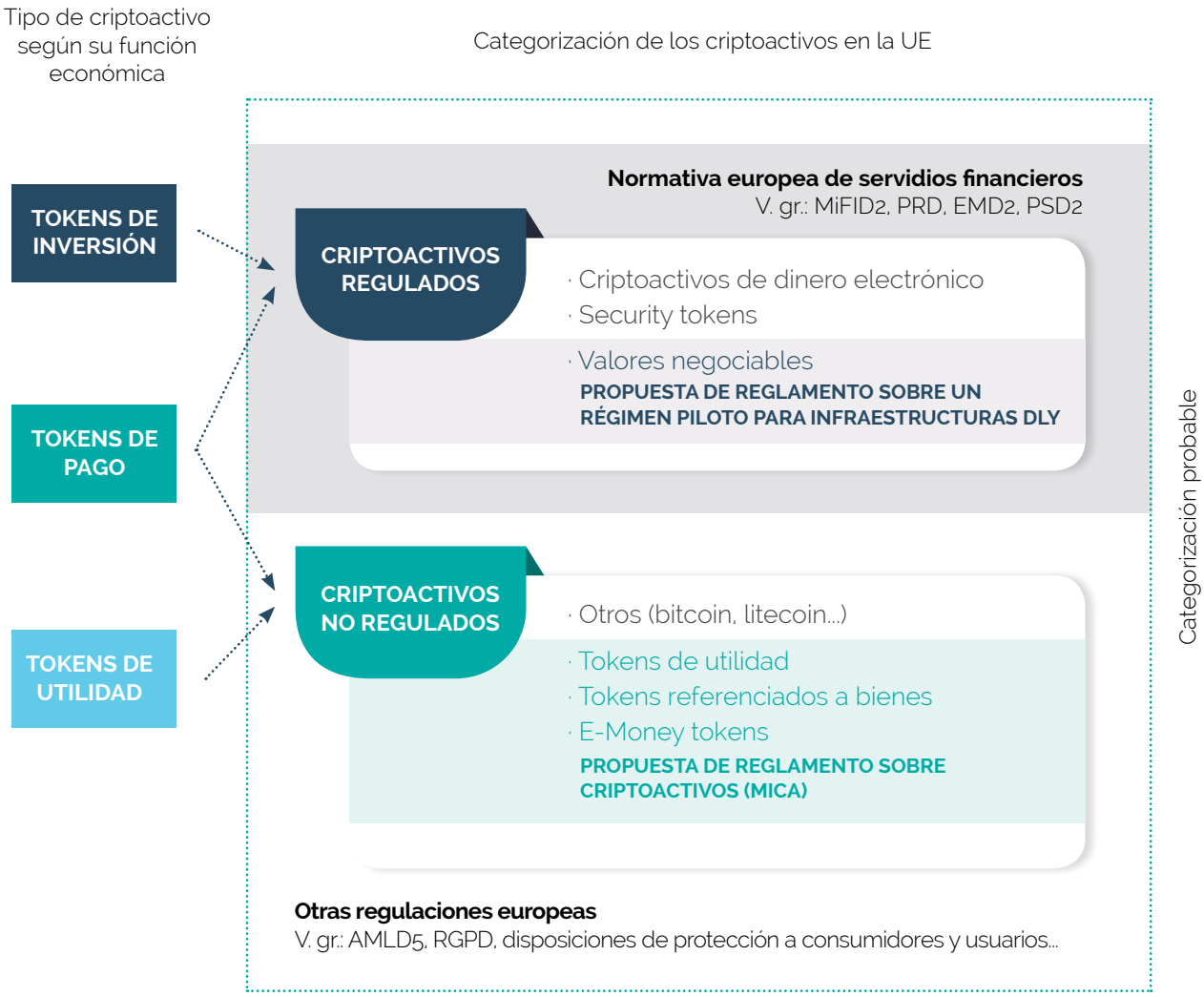
Sobre esta base, la Consulta de la CE, teniendo en cuenta las consideraciones formuladas por otras instituciones de la UE, clasificó los criptoactivos en "regulados" y "no regulados".

---

[11] Propuesta de un reglamento sobre un régimen piloto para infraestructuras de mercado basadas en tecnologías de registro distribuido. Accedido desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1600960374694&uri=COM:2020:594:FIN.

[12] Autoridad Suiza de Supervisión de los Mercados Financieros. (2018), Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs). Accedido desde: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

Capítulo 1. – Categorización básica de criptoactivos en la Consulta de la CE y MiCA.



Nota: este gráfico muestra el marco conceptual de la Consulta de la CE para abordar una clasificación de criptoactivos, a la luz de las definiciones incluidas en las Propuestas de reglamento MiCA y de Régimen Piloto. Téngase en cuenta que esta taxonomía no está establecida en la legislación de la UE.

A. CRIPTOACTIVOS REGULADOS

Los criptoactivos regulados se definen por el hecho de que entran en el ámbito de aplicación del régimen de servicios financieros de la UE. Hay tres tipos de criptoactivos regulados: "criptoactivos de dinero electrónico", "tokens de valores negociables" ("Securitiy token") y "valores negociables sobre DLT".

Según la CE y algunas autoridades financieras de la UE, los criptoactivos regulados normalmente abarcarán los criptoactivos que funcionan como tokens de inversión. En algunos casos, los tokens de pago, por ejemplo, algunas "stablecoins", también podrían entrar en esta categoría, como se explica más adelante. Por otra parte, es probable que los tokens de utilidad no cumplan las condiciones para funcionar como Security token o como criptoactivos de dinero electrónico y, por lo tanto, normalmente se encontrarán en el ámbito de los criptoactivos no regulados. Por esta razón, la Propuesta de Reglamento MiCA incluye a los tokens de utilidad en su ámbito de aplicación, como se verá más tarde.

Criptoactivos de dinero electrónico

La directiva sobre dinero electrónico ("EMD2", por sus siglas en inglés)[13] establece las normas en materia de prácticas comerciales y supervisión de las instituciones de dinero electrónico. Un criptoactivo se calificará como dinero electrónico en la medida en que satisfaga cada elemento de la definición legal en EMD2:

- Valor monetario almacenado por medios electrónicos o magnéticos;
- que representa un crédito sobre el emisor;
- se emite al recibo de fondos con el propósito de efectuar operaciones de pago;
- y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.

A los efectos de este trabajo, denominaremos a este tipo de criptoactivo como "criptoactivos de dinero electrónico".

Desde un punto de vista práctico, la autoridad financiera del Reino Unido (Finantial Conduct Authority, "FCA" por sus siglas en inglés) sostuvo en su "Guía sobre criptoactivos" ("Informe de la FCA") que es poco probable que tokens de pago como el bitcoin, el ether y otros representen dinero electrónico porque, entre otras cosas, no suelen emitirse de forma centralizada al recibir los fondos, ni representan un crédito contra un emisor[14]. Además, la FCA considera que es poco probable que los criptoactivos que establecen un nuevo tipo de unidad de cuenta, en lugar de representar fondos fiduciarios, lleguen a ser dinero electrónico a menos que el valor de la unidad esté vinculado a una moneda de curso legal[15].

Es interesante señalar que la Propuesta de Reglamento MiCA ha incluido una nueva categoría de criptoactivo denominado "e-money token", distinta de los criptoactivos que encajan en la

definición de dinero electrónico bajo EMD2. En la letra B de esta sección se exploran las diferencias entre ambas definiciones.

Security tokens

La segunda directiva relativa a los mercados de instrumentos financieros ("MIFID2", por sus siglas en inglés)[16] contiene una lista de los instrumentos que se consideran "instrumentos financieros" bajo su ámbito de aplicación, entre los que figuran, entre otros, los "valores negociables", los "instrumentos del mercado monetario", las "participaciones y acciones en instituciones de inversión colectiva" y diversos instrumentos derivados. En función de sus características específicas, los criptoactivos podrían calificarse como algunos de estos instrumentos, especialmente como valores negociables. De acuerdo con la categorización de

[13] *Directiva sobre dinero electrónico (2009/110/EC).*

[14] *Financial Conduct Authority (FCA). (2019), Guidance on Cryptoassets, July version. Accedido desde: https://www.fca.org.uk/publication/consultation/cp19-03.pdf, p. 31.*

[15] *Ibid., p. 45.*

[16] *Directiva relativa los mercados de instrumentos financieros II (2014/65/EU).*

la Consulta de la CE, los criptoactivos que se califican como "valores negociables"[17] u otros instrumentos financieros se denominan "Security tokens".

La mayoría de los participantes en la encuesta de la AEVM a las autoridades financieras de los estados miembros de la UE estuvieron de acuerdo en que la vinculación al token de derechos de participación en el reparto de ganancias (ya sea junto con derechos de propiedad o de voto o sin ellos) era suficiente para que un criptoactivo constituyera un valor negociable, siempre que el criptoactivo fuera libremente negociable y no funcionara como instrumento de pago[18].

Notablemente, la AEVM excluyó de la encuesta los tokens de pago puros (como bitcoin, ether y litecoin) sobre la base de que es poco probable que se puedan calificar como instrumentos financieros. Asimismo, las autoridades financieras de los estados miembros mostraron consenso en cuanto a la conveniencia de excluir los tokens de utilidad puros del perímetro de la regulación financiera vigente en la UE sobre la base de que los derechos que transmiten parecen estar demasiado alejados de la estructura financiera y monetaria de un valor negociable o de un instrumento financiero[19].

La misma línea de pensamiento fue seguida por el Grupo de Interés de Valores y Mercados ("SMSG", por sus siglas en inglés) en un informe a la AEVM en octubre de 2018[20]. La organización llega a la conclusión de que los tokens de pago no están actualmente cubiertos por MIFID2 ni por otras normativas financieras. No obstante, el SMSG advierte que los tokens de pago se consideran cada vez más como activos de inversión que dan lugar a riesgos similares a los de los mercados de capitales (cuestiones de protección a inversores y de abuso del mercado), proponiendo incluso incluir estos criptoactivos en la definición de instrumento financiero[21].

En el caso de los tokens de utilidad, el SMSG opina que tienen el potencial de convertirse en activos de inversión solamente cuando son negociables. Por el contrario, cuando solo pueden utilizarse en relación con el emisor, no quedarían comprendidos en el ámbito de aplicación de la normativa de servicios financieros, a menos que pudieran calificarse como dinero electrónico[22].

---

[17] Valores negociables se define en el punto 44 del artículo 4.1. MIFID2 como "las categorías de valores que son negociables en el mercado de capitales, con excepción de los instrumentos de pago, como: a) acciones de sociedades y otros valores equiparables a las acciones de sociedades, asociaciones u otras entidades, y certificados de depósito representativos de acciones; b) bonos y obligaciones u otras formas de deuda titulizada, incluidos los certificados de depósito representativos de tales valores; c) los demás valores que dan derecho a adquirir o a vender tales valores negociables o que dan lugar a una liquidación en efectivo, determinada por referencia a valores negociables, divisas, tipos de interés o rendimientos, materias primas u otros índices o medidas.

[18] Autoridad Europea de Valores y Mercados. (2019), Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p. 5.

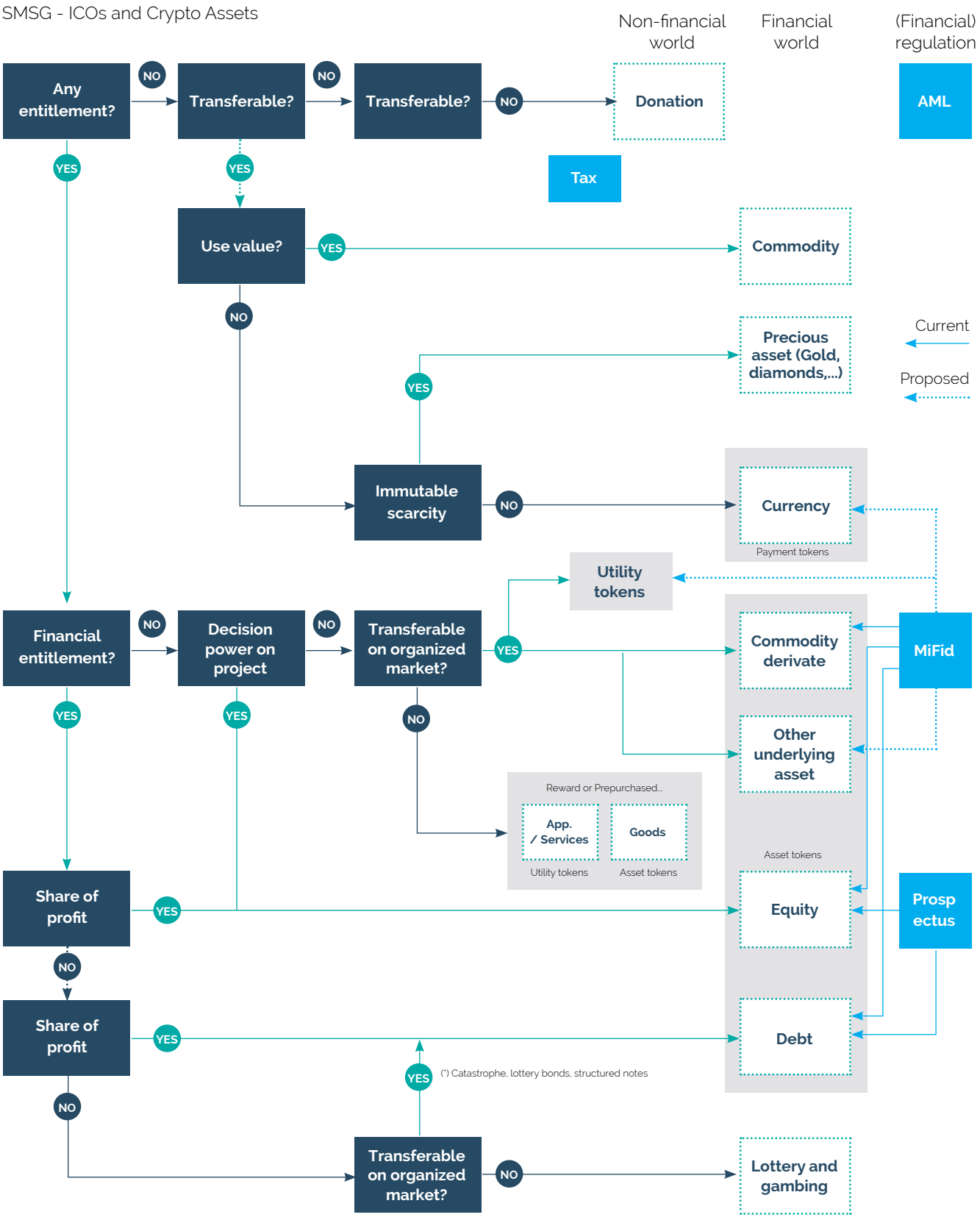
[19] Idem, p. 20.

[20] Grupo de Interés de Valores y Mercados. (2018), Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets. Accedido desde: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.

[21] Ibid., p. 13-14.

[22] Idem.

Capítulo 2. – Aplicabilidad de la normativa sobre servicios financieros a los criptoactivos, según SMSG



Valores negociables sobre DLT

La Propuesta de Régimen Piloto, en su artículo 5, define como "valores negociables sobre DLT" ("DLT transferable securities") aquellos "valores negociables" en el sentido del artículo 4.1.44), letras (a) y (b), de la Directiva 2014/65/ EUMIFID2, que se emitan, registren, transfieran y almacenen mediante una DLT.

Los valores negociables sobre DLT son, por lo tanto, un subconjunto específico de Security token, coincidente con la definición de valor negociable según MIFID2. La Propuesta de Régimen Piloto crea esta categoría de criptoactivo para limitar el tipo de instrumentos financieros que podrían admitirse a negociación en "infraestructuras de mercado DLT"[23]. Como tendremos oportunidad de explorar más adelante, solo ciertos valores negociables sobre DLT pueden ser admitidos a negociación en estas infraestructuras.

B. CRIPTOACTIVOS NO REGULADOS

Los criptoactivos no regulados son aquellos que caen fuera del perímetro de la regulación de servicios financieros de la UE. Esta categoría abarca una amplia variedad de criptoactivos, normalmente de utilidad y de pago, así como criptoactivos con una función híbrida.

Obsérvese que el término no regulado no significa que estos criptoactivos queden fuera del ámbito de cualquier normativa de la UE, sino simplemente que el marco de regulación de los servicios financieros no les es aplicable. Por ejemplo, los tokens de pago normalmente entrarán en la definición de "moneda virtual" y, por lo tanto, estarán sujetas a las disposiciones sobre blanqueo de capitales[24]. Del mismo modo, la venta de criptoactivos no regulados a un público calificado como "consumidores" desencadenará la aplicación del paquete de medidas de la UE sobre protección al consumidor. Las consideraciones fiscales son también un ángulo jurídico relevante al analizar las consecuencias jurídicas de operar con criptoactivos.
Fuera del perímetro de la normativa financiera (es decir, cuando los criptoactivos no encajan en la definición de instrumentos financieros o de dinero electrónico), la Propuesta de Reglamento MiCA definiría, entre otros, términos relevantes para el desarrollo de una taxonomía de criptoactivos para la UE, incluyendo la definición de "criptoactivo", tokens de utilidad, "e-money tokens" y los "tokens referenciados a activos".

La definición de criptoactivo en esta propuesta de Reglamento[25] es lo más amplia posible para capturar todos los tipos de criptoactivos que actualmente quedan fuera del alcance de la legislación de servicios financieros de la UE y garantizar que el Reglamento no quede rápidamente obsoleto y se mantenga al día con la innovación y la tecnología desarrollos en el sector. Más allá de la definición general de criptoactivos, la Propuesta de Reglamento MiCA distingue entre tres subcategorías de criptoactivos que están sujetos a requisitos específicos: tokens de utilidad, e-money tokens y los tokens referenciados a activos.

Tokens de utilidad

La Propuesta de Reglamento MiCA define token de utilidad como "un tipo de criptoactivo que está destinado a proporcionar acceso digital a una aplicación, servicios o recursos disponibles en un registro distribuido y que son aceptados solo por el emisor de ese token para otorgar acceso a dicha aplicación, servicios o recursos disponibles".

El hecho de que la Propuesta de Reglamento MiCA decidiera definir este tipo de activo como una subcategoría específica y no definir tokens de pago podría servir de indicativo de que este

[23] El Artículo 2.2 de la Propuesta de Régimen Piloto establece que una "infraestructura de mercado DLT" significa, o bien un sistema multilateral de negociación basado en DLT, o bien un depositario central de valores basado en DLT, como se define en los artículos 2.3 y 4 del mismo Reglamento.

[24] Véase el artículo 3.18) de la quinta directiva relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo (Directiva 2018/843/EU).

[25] Criptoactivo según la Propuesta de Reglamento MiCA, artículo 3.1.b), significa "una representación digital de valor o derechos, que puede transferirse y almacenarse electrónicamente, utilizando un registro distribuido o tecnología similar".

Reglamento excluye los tokens de pago de su alcance. Así sería en la medida en la que el criptoactivo en cuestión no encaje en las categorías de e-money tokens o tokens con referencia a activos. Esto dejaría fuera del perímetro de la Propuesta de Reglamento MiCA a criptoactivos como bitcoin, litecoin, bitcoin cash u otros proyectos que no tratan de mantener estable el valor del criptoactivo.

E-money tokens

Según la Propuesta de Reglamento MiCA, un e-money token es un "tipo de criptoactivo cuyo propósito principal es ser utilizado como medio de intercambio y que pretende mantener un valor estable al estar denominado en (unidades de) una moneda de curso legal"[26]. La Propuesta de Reglamento MiCA determina que los criptoactivos que puedan ser clasificados como dinero electrónico bajo EMD2 pero no como e-money tokens bajo la Porpuesta de Reglamento MiCA, estarán fuera del perímetro de MiCA.

A pesar de sus similitudes, existen algunas diferencias entre el dinero electrónico en EMD2 y los e-money token. Por ejemplo, los titulares de dinero electrónico en virtud de EMD2 siempre cuentan con un derecho de crédito frente a una institución de dinero electrónico y tienen por contrato el derecho de canjear su dinero electrónico en cualquier momento por dinero de curso legal al valor nominal de la moneda en la que se denomine el criptoactivo. Por el contrario, algunos e-money tokens no brindan a sus poseedores este derecho contra los emisores del token y podrían quedar fuera del alcance de EMD2. Además, otros e-money tokens no brindan la posibilidad de canjear el token por la moneda que denominan o limitan el período de canje.

La razón detrás de definir esta nueva categoría de e-money tokens, en oposición a los criptoactivos que caen dentro del alcance de EMD2, es crear una definición amplia capaz de capturar todos los tipos de criptoactivos que se denominan en una sola moneda de curso legal y en prevenir el arbitraje regulatorio con las disposiciones de EMD2 o la elusión de las reglas de la UE[27].

Tokens referenciados a activos

Un token referenciado a activos significa un "tipo de criptoactivo cuyo propósito principal es ser utilizado como medio de intercambio y que pretende mantener un valor estable refiriéndose al valor de varias monedas fiduciarias, una o varias materias primas o una o varias criptoactivos, o una combinación de dichos activos".

---

[26] Véase el artículo 3.1.d de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre criptoactivos. Accedido desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN.

[27] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre criptoactivos. Accedido desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN, p. 16-17.

De las dos últimas definiciones, parece claro que la Propuesta de Reglamento MiCA tiene su ojo puesto en las stablecoins. Sin embargo, persisten complejidades relevantes al intentar encajar las stablecoins en instituciones jurídicas existentes, incluyendo todas las categorías repasadas antes (criptoactivos de dinero electrónico, Security token, tokens de utilidad, e-money tokens y tokens referenciados a activos).

La Asociación Europea de Bancos Cooperativos ("EACB", por sus siglas en inglés) respondió que "no está en absoluto claro lo que son [las stablecoins] por el momento", y que bien podrían ser tanto simples etiquetas al servicio de estrategias de marketing, como dinero electrónico o como algún tipo de fondo tokenizado con activos mantenidos por una entidad de custodia o un depositario[28].

Otros participantes han declarado que los criptoactivos con materias primas como subyacente comparten las mismas características que los derivados de materias primas, por ejemplo, el SMSG[29]. La AEVM clasificó los stablecoins como similares a valores referenciados a materias primas negociables y, por lo tanto, podrían formar parte de la definición de valores negociables en virtud de MIFID2[30]. Además, en octubre de 2019, el G7 publicó un documento sobre stablecoins[31] que parece seguir un enfoque similar al de la AEVM.

III. CRIPTOACTIVOS REGULADOS: MODIFICACIONES EN EL MARCO JURÍDICO FINANCIERO DE LA UE PARA SU APLICACIÓN EFECTIVA SOBRE CRIPTOACTIVOS

A pesar de que la legislación financiera de la UE no se redactó teniendo en cuenta los criptoactivos, varias instituciones jurídicas existentes, como el dinero electrónico o los valores negociables, pueden servir hoy en día para incorporar algunos criptoactivos al marco jurídico de la UE, como hemos visto.

Sin embargo, la aplicación de la legislación de la UE en el ámbito de los criptoactivos no está exenta de dificultades. En primer lugar, existe la evidente dificultad de subsumir creaciones totalmente innovadoras en instituciones jurídicas ya establecidas que no se desarrollaron con los criptoactivos en mente. Además, algunas disposiciones actuales pueden inhibir la posibilidad de utilizar tecnologías DLT. Por último, algunos aspectos cruciales no están armonizados a nivel de la UE y algunos estados miembros de la UE están adoptando enfoques diferentes para casos similares, lo que da lugar a fragmentación normativa que a la larga puede dar lugar al arbitraje normativo. La Consulta de la CE exploró estas dificultades y solicitó opiniones para solucionarlas.

En esta sección se repasan dos de las principales dificultades para aplicar el marco regulador existente para servicios financieros a los criptoactivos y se concluye con las posibles medidas reguladoras previstas por la CE para hacer frente a estas dificultades.

A. Aplicación imprecisa del marco normativo e incertidumbre jurídica

Cuando se considera que los criptoactivos entran dentro del perímetro de la normativa financiera de la UE, no siempre es fácil determinar cómo debe aplicarse esta normativa. Esta circunstancia supone un reto para todos los agentes implicados (incluidos los supervisores financieros, las empresas de inversión en criptoactivos y los inversores) y genera inseguridad jurídica. Por ejemplo, los inversores pueden tener dificultades para determinar si tienen derecho a protección legal, mientras que muchos participantes en el mercado pueden no tener claras las normas que deben cumplir, si es que deben cumplir alguna, para asegurarse de que las actividades que realizan se ajustan a la normativa vigente.

---

[28] Véase la p. 58 de la respuesta de la EACB a la Consulta.

[29] Grupo de Interés de Valores y Mercados. (2018), Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets. Accedido desde: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf, p. 11.

[30] Autoridad Europea de Valores y Mercados. (2019). Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.19.

[31] G7 Grupo de trabajo en stablecoins. (2019), Investigating the impact of global stablecoins. Accedido desde: https://www.bis.org/cpmi/publ/d187.pdf.

Esto queda especialmente claro cuando los aspectos novedosos en torno de los criptoactivos ponen en entredicho la capacidad del marco actual para servir como una solución normativa eficaz. Ejemplos claros de ello pueden ser las stablecoins, las plataformas híbridas, los criptoactivos híbridos y las casas de cambio descentralizadas.

B. Fragmentación y arbitraje normativo

En los casos en los que los criptoactivos puedan calificarse como valores negociables u otros tipos de instrumentos financieros en virtud de MIFID2, sus emisores y/o las empresas que prestan servicios/actividades de inversión con estos instrumentos quedarán probablemente sometidas a un conjunto amplio de normas financieras de la UE, entre ellas el reglamento sobre el folleto informativo ("PR", por sus siglas en inglés)[32], la directiva sobre transparencia, MIFID2, la directiva sobre abuso de mercado, el reglamento sobre la venta en corto y otras[33]. Las actividades relativas a los Security tokens se calificarían como servicios/actividades de inversión y las transacciones de Security tokens admitidas a cotización o negociadas en un centro de negociación quedarían comprendidas en diversas disposiciones financieras[34].

A pesar del marco común establecido por MIFID2, la clasificación efectiva de un criptoactivo como instrumento financiero es responsabilidad de las autoridades financieras de cada estado miembro y dependerá de la aplicación nacional específica de la legislación de la UE basada en la información y las pruebas que se proporcionen a cada autoridad financiera[35]. Por ejemplo, la definición de instrumento financiero se ha transpuesto de manera diferente en los diferentes estados miembros de la UE, de modo que mientras algunos emplean una lista cerrada – numerus clausus – de valores negociables, otros utilizan listas abiertas – numerus apertus. En consecuencia, los estados miembros de la UE podrían llegar a conclusiones diferentes al evaluar la calificación jurídica de un determinado criptoactivo como Security token, lo que plantea nuevos problemas para la adopción de un marco normativo y de supervisión común en toda la UE. Además, la situación actual pone en tela de juicio la capacidad de las autoridades financieras de los estados miembros para interpretar el marco normativo de forma cohesionada, lo que aumenta el riesgo de arbitraje normativo.

Por ejemplo, Alemania ha enmendado su ley bancaria para implementar la quinta directiva sobre blanqueo de capitales en el país y ha considerado que los criptoactivos con fines de pago deben ser considerados instrumentos financieros si se ajustan a la siguiente definición:

- Una representación digital de valor que;
- no ha sido emitida ni garantizada por un banco central o un organismo público;
- no tiene el estatus legal de moneda o dinero pero;
- sobre la base de un acuerdo o práctica en marca;
  - es aceptado por personas físicas o jurídicas;
  - como medio de intercambio o pago; o
  - sirve para propósitos de inversión; y
- puede ser transferido, almacenado y comercializado por medios electrónicos.

La ley bancaria de Alemania excluye de esta definición a los criptoactivos que funcionan legalmente como dinero electrónico, así como a ciertos activos monetarios[36].

Otro ejemplo puede ser el de los Países Bajos, donde los criptoactivos son considerados como

---

[32] Reglamento sobre el folleto informativo (2017/1129/EU).

[33] Autoridad Europea de Valores y Mercados. (2019). Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[34] Comisión Europea. (2019), Consultation Document on an EU framework for markets in crypto-assets. Accedido desde https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf, p. 29.

[35] Autoridad Europea de Valores y Mercados. (2019). Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[36] Autoridad Federal de Supervisión Financiera (BAFIN). (2020), Guidance Notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG). Accedido desde: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html.

valores por la autoridad financiera nacional si son transferibles y negociables en los mercados financieros y si representan: i) una acción o un derecho o instrumento equivalente; ii) un bono u otro instrumento de deuda; o iii) cualquier otro instrumento que pueda convertirse en una acción, un bono o un equivalente o que pueda liquidarse en efectivo. Nótese que la ley holandesa enumera las tres categorías anteriores como una lista cerrada y exhaustiva – numerus clausus -, en contraste con la definición de la MIFID2, que utiliza una lista no exhaustiva, abierta a otro tipo de valores – numerus apertus. En consecuencia, la capacidad de la autoridad financiera holandesa para interpretar qué es un Security token se ve considerablemente restringida en comparación con otros estados miembros de la UE[37].

C. Posibles medidas de regulación

En los non-papers mencionados anteriormente, la CE entendió que los problemas tratados en esta sección podrían abordarse mediante una combinación de medidas legislativas y no legislativas[38]. En particular, la CE indica tres opciones a considerar:

- medidas no legislativas que proporcionarían orientación sobre la forma en que la legislación vigente se aplica a los criptoactivos;
- cambios legislativos específicos que eliminen las disposiciones que actúan como un obstáculo para la emisión, la negociación y post-negociación de Security tokens; o
- un régimen piloto para las infraestructuras de mercados DLT que operen con criptoactivos que encajan en la definición de instrumento financiero.

C1. Orientación sobre la forma en la que la legislación vigente se aplica a los criptoactivos

En los non-papers se propuso una comunicación interpretativa en la que la CE exponga su opinión sobre las características que deberían tener los criptoactivos para ser considerados instrumentos financieros o dinero electrónico bajo el marco vigente. Como medida adicional, los non-papers mencionaron que la CE podría orientar sobre la forma en que la legislación sectorial vigente (MIFID2, PR…) aplicaría a los criptoactivos que encajen en la definición de instrumento financiero[39].

C2. Posibles enmiendas específicas a la legislación vigente sobre servicios financieros

En los casos en que las disposiciones de la legislación sectorial obstaculicen o impidan claramente el uso de tecnologías de registro distribuido o de Security tokens, o cuando no se pueda garantizar la aplicación adecuada de la legislación en el entorno DLT, la CE podrá presentar enmiendas específicas para abordar estas cuestiones. Es posible que estas enmiendas no requieran cambios de nivel 1, sino que podrían requerir modificaciones de nivel 2, las cuales podrían también realizarse al revisar la normativa en cuestión[40].

Esta iniciativa podría incluir una enmienda específica de la noción de instrumento financiero en el marco de MIFID2, para garantizar que dicho instrumento pueda emitirse sobre una tecnología DLT

Estas enmiendas permitirían el uso de redes centralizadas y de redes DLT permisionadas. En particular, esta iniciativa podría incluir una enmienda específica de la noción de instrumento financiero en el marco de MIFID2, para garantizar que dicho instrumento pueda emitirse sobre una tecnología DLT[41].

---

[38] Comisión Europea. (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Accedido desde https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf, p.4.

[39] Ibid.

[40] Ibid.

[41] Comisión Europea. (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Accedido desde https://drive.google.com/file/d/1Z-Bl_YSUcKblJCrsOtoQk66z4jtd7Dvkj/view, p.1.

Además, la Propuesta de Régimen Piloto indica que la CE tiene previsto publicar una directiva que modifique varias normativas financieras[42], incluida MIFID2, para permitir que los sistemas multilaterales de negociación basados en DLT ("SMN DLT")[43] puedan solicitar una exención de la obligación de intermediación (es decir, la obligación de solo admitir como miembros o participantes a entidades de servicios de inversión, instituciones de crédito y otras personas que tengan un nivel acreditado de experiencia en trading), de tal modo que puedan aceptar a clientes minoristas. En este sentido, a diferencia de los SMN tradicionales, muchas plataformas de negociación de criptoactivos ofrecen un acceso no intermediado y proporcionan acceso directo a clientes minoristas.

C3. Propuesta de reglamento relativo a un régimen piloto para infraestructuras de mercado basadas en tecnologías de registro distribuido

En la versión de julio de los non-papers, la CE observó que hay una falta de infraestructura de mercado en el ámbito DLT, ya que la incertidumbre jurídica desalienta el establecimiento de centros de negociación o de depositarios centrales de valores ("DCV", por sus siglas en inglés)[44]. Según los non-papers, esta infraestructura permitiría la negociación y liquidación de criptoactivos, el desarrollo de mercados secundarios de Security tokens para apoyar el incipiente mercado primario y crear las condiciones para que estos mercados escalen.

Para resolver esta cuestión, la CE ha propuesto un régimen piloto temporal como posible solución, como parte de su propuesta para un marco de la UE sobre criptoactivos.

El régimen piloto funcionaría como un sandbox abierto por un período de hasta seis años, durante el cual proyectos de infraestructuras de mercado DLT puedan operar exentas de algunos requisitos específicos de la legislación de servicios financieros de la UE. El objetivo es eliminar temporalmente ciertos obstáculos regulatorios que podrían estar impidiendo el desarrollo de infraestructuras de mercado basadas en DLT, permitiendo así tanto a los participantes del mercado como a los reguladores ganar experiencia y explorar los riesgos que plantea esta infraestructura.

Una infraestructura de mercado basada en DLT funcionaría como un SNM o como un DCV pero en un entorno DLT. Los agentes que operen esta infraestructura tendrían que obtener una nueva autorización de su autoridad financiera, sobre la autorización como entidad de servicios de inversión u operador de mercado (en el caso de los SMN DLT) o como DCV (en el caso de DCV DLT).

Durante el periodo de prueba, la infraestructura del mercado basada en DLT sólo estaría autorizada a admitir a cotización o a registrar en el libro de contabilidad instrumentos financieros simples (es decir, acciones y bonos) que no sean líquidos. A su vez, los participantes pueden solicitar exenciones cuando operan, sobre todo la posibilidad de admitir inversores minoristas en su base de clientes, eliminando así la obligación de intermediación a través de empresas de inversión, entidades de crédito y otras personas con la experiencia necesaria.

Las autoridades financieras de los estados miembros estarían facultadas para imponer medidas correctivas a la infraestructura del mercado DLT y para retirar el permiso en algunas circunstancias. La AEVM cumpliría una función de coordinación entre las autoridades competentes.

La Propuesta de Régimen Piloto establece que, después de un período de cinco años a partir de la entrada en vigor del Reglamento, la AEVM debe informar a la CE sobre este régi-

[42] Consúltese, por ejemplo, el considerando 17 del Reglamento de Régimen Piloto.

[43] De acuerdo con el artículo 2.3 de la Propuesta de Régimen Piloto, un "SMN DLT" significa un sistema multilateral de negociación (según se define en el artículo 4.1.22) MIFID2), operado por una entidad de servicios de inversión o un operador de mercado, que solo admite a negociación valores negociables sobre DLT.

[44] Un depositario central de valores es persona jurídica que gestione un sistema de liquidación de valores, de conformidad con el reglamento 909/2014.

men piloto, incluidos los beneficios potenciales vinculados al uso de DLT, los riesgos planteados y las dificultades técnicas. En función de las conclusiones del informe de la AEVM, la CE debería informar al Consejo y al Parlamento Europeo. Este informe debe evaluar los costos y beneficios de alargar la aplicación de este régimen, extender este régimen a otros tipos de instrumentos financieros, hacer que este régimen sea permanente con o sin modificaciones, traer modificaciones a la legislación de servicios financieros de la UE o finalizar este régimen.

IV. CRIPTOACTIVOS NO REGULADOS: UN RÉGIMEN JURÍDICO A MEDIDA

A. Introducción

En el Informe de la AEVM se menciona que la mayoría de criptoactivos en circulación probablemente no cumplen los requisitos para ser considerados instrumentos financieros en el marco de MIFID2 y que, por lo tanto, es probable que queden fuera de las normas vigentes sobre servicios financieros de la UE[45]. En consecuencia, los consumidores e inversores no se beneficiarán de las salvaguardias previstas en esas normas y, al mismo tiempo, no podrán distinguir fácilmente si los criptoactivos disponibles en los centros de negociación están dentro del marco jurídico financiero de la UE.

Además, algunos estados miembros de la UE han aplicado o están considerando la posibilidad de aplicar regímenes a medida para criptoactivos que no reúnen las condiciones para ser instrumentos financieros, con el notable ejemplo de Francia y Malta[46], situación que contribuye a la fragmentación normativa en la UE.

Con eso en mente, la Consulta de la CE también recabó opiniones para evaluar si regular los criptoactivos no regulados podría ser beneficioso en este momento para acabar proponiendo la Propuesta de Reglamento MiCA.

B. Propuesta de Reglamento relativa a los mercados de criptoactivos

La Propuesta de Reglamento MiCA (Markets in Crypto-Assets Regulation o "MiCA") ha establecido requisitos armonizados a nivel de la UE para los emisores que deseen ofrecer criptoactivos en toda la UE y proveedores de servicios sobre criptoactivos que deseen solicitar una autorización para prestar sus servicios en el mercado único, cuando estos criptoactivos no encajen en la defininión de intrumento financiero. Esta iniciativa sustituiría a los marcos nacionales existentes aplicables a los criptoactivos no cubiertos por la legislación vigente de la UE sobre servicios financieros.

B1. Requisitos sobre emisores

En relación con la emisión de criptoactivos en la UE, la Propuesta de Reglamento MiCA establece requisitos para emisores de:

- criptoactivos (con la mira especialmente puesta en tokens de utilidad);
- tokens referenciados a bienes; y
- e-money tokens.

En relación con la emisión de criptoactivos, la Propuesta de Reglamento MiCA regula la publicación de un whitpaper o documento informativo armonizado con declaraciones obligatorias (descripción detallada del emisor, el proyecto y el uso previsto de los fondos, las condiciones

---

[45] Autoridad Europea de Valores y Mercados. (2019). Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[46] En Francia, la ley PACTE, por sus siglas en francés, ha creado un marco específico para la oferta de tokens de utilidad al público y para regular ciertos aspectos, como los riesgos operativos y de seguridad, los mecanismos de control interno, la resiliencia de los sistemas informáticos o el conflicto de intereses, para diferentes proveedores de servicios sobre criptoactivos, en aquellos casos en los que los criptoactivos no encajan en la definición de instrumento financiero de MIFID2. El régimen es opcional, lo que significa que los prestadores de servicios no tendrán que cumplir con sus normas y requisitos a menos que decidan opten por someterse a él, punto a partir del cual deberán cumplir en su totalidad. En otras palabras, esta configuración legal ofrece a los proveedores de servicios sobre criptoactivos ganar en seguridad jurídica a cambio de asumir ciertos costes para el cumplimiento regulatorio. Este enfoque novedoso ha sido alabado y criticado, siendo la voz más destacada entre las críticas la de AEVM, que aunque comprende la intención de apoyar estos instrumentos, destaca que este tipo de iniciativas no ayudan a proporcionar un marco homogéneo en toda la UE.

En Malta, el legislador ha adoptado tres leyes relacionadas con DLT, que entraron en vigor el 1 de noviembre de 2018: (i) la Ley de Activos Financieros Virtuales, (ii) la Ley de la Autoridad de Innovación Digital de Malta, y (iii) el Acuerdo de Tecnología Innovadora y Ley de Servicios. Estas tres leyes introducen, entre otras medidas, un requisito para que los emisores de activos financieros virtuales elaboren y pongan a disposición un whitepaper, requisitos de licencia para proveedores de servicios financieros virtuales como corredores, reglas de conducta comercial para titulares de licencias y ciertos requisitos sobre blanqueo de capitales para titulares de licencias.

de la oferta, los derechos y obligaciones vinculados a las criptoactivos y los riesgos). Quedarán exentas de este requisito las ofertas pequeñas (de valor inferior a 1 millón de euros en un período de doce meses), las ofertas dirigidas a inversores cualificados, tal como se definen en el PR y otros supuestos listados en el artículo 4.2 de la Propuesta. Este documento no deberá ser autorizado por las autoridades financieras de los estados miembros, aunque deberá ser notificado antes de su publicación.

Será responsabilidad del emisor justificar ante las autoridades financieras de los estados miembros por qué el criptoactivo en cuestión no reúne las condiciones para ser un instrumento financiero en virtud de MIFID2 o como dinero electrónico en virtud de EMD2.

Será responsabilidad del emisor justificar ante las autoridades financieras de los estados miembros por qué el criptoactivo en cuestión no reúne las condiciones para ser un instrumento financiero

Los emisores de tokens referenciados a bienes tendrán que obtener autorización antes de realizar una oferta, a menos que la cantidad promedio de estos tokens no supere los 5 millones de euros durante un período de 12 meses o que la oferta se dirija solo a inversores cualificados. Además, tendrán que cumplir una serie de requisitos, por ejemplo, establecerse como entidad jurídica en la UE, revelar los derechos vinculados al token, incluida toda posible reclamación directa sobre el emisor o la reserva de activos, y están obligados a publicar un whitepaper con declaraciones obligatorias adicionales a las exigidas en el caso de las emisiones regulares de criptoactivos. En este caso, el whitepaper tendrá que ser aprobado por las autoridades financieras de los estados miembros, que se encargarán de la autorización y la supervisión permanente de los emisores de tokens referenciados a bienes.

En cuanto a los emisores de e-money tokens, la Propuesta de Reglamento MiCA impone la obligación de que estos tokens sean emitidos por una institución de crédito autorizada en virtud del Reglamento (UE) 2013/575 o por una institución de dinero electrónico en virtud de EMD2. Vale la pena señalar que deberán otorgar a sus usuarios el derecho de canjear el token en cualquier momento y al valor nominal de la moneda en la que se denomina.

B2. Proveedores de servicios con autorización previa

En relación con los proveedores de servicios relacionados con criptoactivos, la Propuesta de Reglamento MiCA regularía los siguientes servicios:

- custodia y administración de criptoactivos en nombre de terceros;
- funcionamiento de una plataforma de comercio de criptoactivos;
- intercambio de criptoactivos contra moneda fiduciaria mediante el uso de capital propio;
- intercambio de criptoactivos contra otros criptoactivos utilizando capital propio;
- recepción y transmisión de órdenes sobre criptoactivos en nombre de terceros;
- ejecución de órdenes en nombre de terceros;
- colocación de criptoactivos;
- asesoramiento sobre criptoactivos; y
- transacciones de pago con stablecoins.

Se prevé que las autoridades financieras de los estados miembros se encarguen de la autorización de los proveedores de servicios sobre criptoactivos. Una vez autorizados, se les permitiría prestar sus servicios en toda la Unión.

IV. CONCLUSIÓN

Como se ha examinado a lo largo del presente documento, hay razones que justificarían la adopción de medidas para garantizar que los

criptoactivos se ajustan adecuadamente al marco normativo vigente de servicios financieros y para regular los riesgos derivados de la emisión y operación con criptoactivos no regulados.

La CE ha puesto sobre la mesa una serie de propuestas interesantes para centrar el debate, con un paquete de medidas legislativas y no legislativas.

En relación con la posibilidad de desarrollar una taxonomía sobre criptoactivos, algunas definiciones importantes podrían incorporarse al acervo jurídico de la UE a través de la Propuesta de Reglamento MiCA, si sale adelante. Adicionalmente, se podría desarrollar una taxonomía de criptoactivos en la UE mediante medidas no legislativas, por ejemplo, mediante directrices de la CE o de las autoridades de la UE para la supervisión financiera, para asegurar una interpretación consistente a lo largo de la UE.

A fin de garantizar que el marco normativo financiero vigente de la UE pueda aplicarse eficazmente a los criptoactivos, la CE propone una combinación de medidas legislativas y no legislativas:

- medidas no legislativas para orientar la forma en que la legislación financiera vigente se aplica a los criptoactivos;
- cambios legislativos específicos que eliminen las disposiciones que actúan como barrera para la emisión, la negociación y la post-negociación de Security tokens; o
- un régimen piloto para las infraestructuras de mercado basadas en DLT para los criptoactivos que encajan en la definición de instrumento financiero.

Por último, la CE ha previsto un régimen jurídico a medida, el reglamento MiCA, para los criptoactivos no regulados, que podría servir para aliviar los problemas derivados de la emisión y operación con estos criptoactivos.

Abreviaturas:

UE – Unión Europea
DLT – tecnología de registro distribuido, por sus siglas en inglés (Distributed Ledger Technology)
AEVM – Autoridad Europea de Valores y Mercados
ABE – Autoridad Bancaria Europea
CE – Comisión Europea
MiCA – Propuesta de Reglamento del Parlamento Europeo y de Consejo sobre criptoactivos
Informe de la AEVM – Advice Initial Coin Offerings and Crypto-Assets
Informe de la ABE – Report with advice for the European Commission on crypto-assets
Consulta de la Comisión Europea – Consultation Document on an EU framework for markets in crypto-assets
AMLD5 – Directiva 2018/843/EU, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE
MIFID2 – Directiva 2014/65/CE, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE
EMD2 – Directiva 2009/110/CE, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE
FCA – Financial Conduct Authority
Informe de la FCA – Guidance on Cryptoassets
AEBC – Asociación Europea de Bancos Cooperativos
PSD2 – Directiva 2015/2366/CE, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE
PR – Reglamento 2017/1129/EU, sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE
SMN – Sistema Multilateral de Negociación
DCV – Depositario Central de Valores

An EU Legal Framework for **Crypto-Assets: Current Status**

Blanca Escribano. José María Chozas.
Lawyers. EY

1. INTRODUCTION

As blockchain-related technologies keep growing around the world, regulators have kept a closed eye on them both to leverage their potential and to help navigating unwanted risks.

Political institutions in the European Union ("EU"), led by the European Commission ("EC"), have been for some time studying the phenomenon and a variety of pan-European public-led initiatives have been brought up since the appearance of Bitcoin. The Fintech Action Plan in 2018[1] paved the route for important works assessing the applicability and suitability of the EU's financial services regulatory framework to crypto-assets[2]. In January 2019, the European Securities and Markets Authority (ESMA") and the European Banking Authority ("EBA"), released reports addressed to the EC – ESMA's advice on ICOs and crypto-assets ("ESMA Report")[3] and EBA's report for the EC on crypto-assets[4] - highlighting a number of regulatory concer-

[1] *European Commission (EC). (2018), Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic And Social Committee and the Committee of the Regions. FinTech Action plan: For a more competitive and innovative European financial sector. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109*

[2] *Crypto-asset is defined in the MiCA Regulation Proposal, article 3(1)(b), as "a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology".*

[3] *European Securities and Markets Authority (ESMA). (2019), Advice Initial Coin Offerings and Crypto-Assets. Retrieved from https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection.*

[4] *European Banking Authority (EBA). (2019), Report with advice for the European Commission on crypto-assets. Retrieved from https://eba.europa.eu/eba-reports-on-crypto-assets.*

ns. Most notably, the reports pointed out that most crypto-assets currently fall outside the EU's financial services regulatory framework, thus not being subject to consumer and investor protection or to market integrity provisions. When crypto-assets do fall within the scope of EU financial legislation, its application to these assets is sometimes not forthright or even some provisions may be capable of hindering the use of blockchain or distributed ledger ("DLT") technologies. Another worth-noting fact is that a number of EU member states have been legislating some aspects related to crypto-assets which are not harmonized at the EU level.

In this context, the EC launched a public consultation ("EC Consultation") on an EU framework for markets in crypto-assets, completed from 19 December 2019 to 19 March 2020[5], stressing the need for "a common approach with member states on cryptocurrencies to ensure [they] understand how to make the most of the opportunities they create and address the new risks they may pose". [6] The EC Consultation was followed by a webinar on 13 May 2020 that showed the EC's intention to regulate, at least to some extent, the intersection between the crypto-asset and the financial space, despite frontal opposition from a number of stakeholders. Following extensive feedback from the industry and regulatory authorities from around the world, the EC issued a "Non-paper[7] on the legislative proposals for an EU framework for markets in crypto-assets" in May 2020,[8] later updated in July 2020,[9] outlining possible actions to develop an EU regulatory framework on crypto-assets.

---

[5] European Commission. (2019), Consultation Document on an EU framework for markets in crypto-assets. Retrieved from https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf.

[6] Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis, 10 September 2019.

[7] A non-Paper is a discussion document designed to stimulate debate on a particular issue without representing the official position of the institution which drafted it.

[8] European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Retrieved from https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf.

[9] European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Retrieved from https://drive.google.com/file/d/1ZBl_YSUcKblJCrsOtoQk66z4jtd7Dvkj/view.

As a result, in September 2020, the EC released two proposed regulations as a first step of its unified framework for crypto-assets: the proposal for a regulation on Markets in Crypto-assets ("MiCA Regulation Proposal")[10] and the proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology ("Pilot Regime Proposal")[11].

With the above in mind, this paper presents the conceptual framework under which the EC tackled the development of pan-EU legislation on crypto-assets and the measures finally proposed to adopt this harmonized framework. This will take us through the following topics:

- **An EU classification for crypto-assets.** The first section will explore a legal taxonomy of tokens in the EU which combines the categorization of crypto-assets presented by the EC Consultation and the token categories laid down in MiCA.
- **Regulated crypto-assets:** amendments to the EU financial services legal framework to be effectively applied to crypto-assets. The second section tackles some of the causes pointed by the EC as the reasons why existing financial legislation might need some tweaks before it is ready to effectively apply to the field of crypto-assets and presents the possible legislative and non-legislative measures that the EC might put in place to solve the issues identified during the EC Consultation.
- **Unregulated crypto-assets:** a bespoke regime. The third section navigates briefly how regulating at the EU level might solve some issues in the space of unregulated crypto-assets and presents briefly the main lines of a regulation designed by the EC to regulate unregulated crypto-assets.

II. AN EU CLASSIFICATION FOR CRYPTO-ASSETS

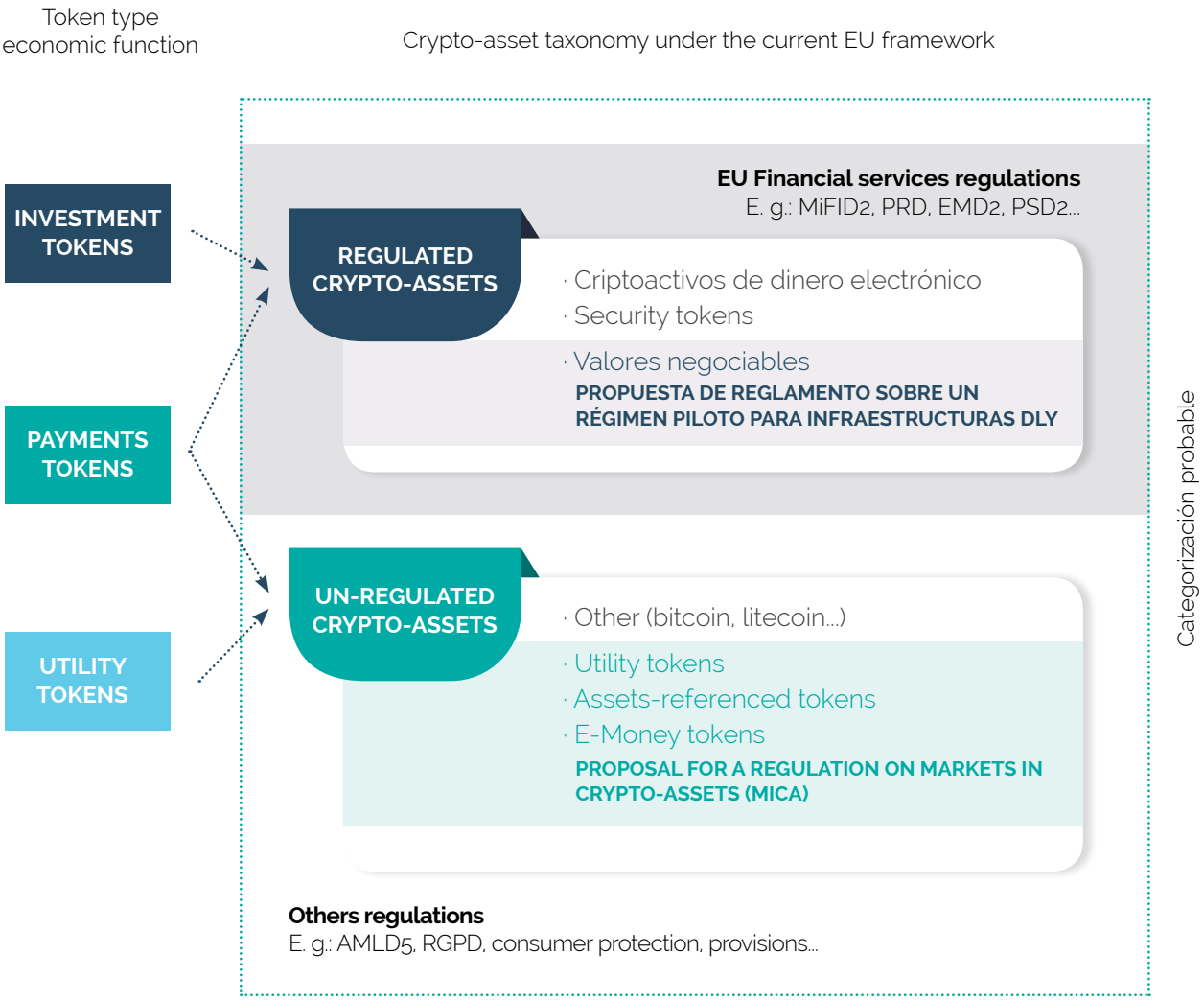
As a starting point, the EC Consultation embraced the well-known Swiss Financial Market Supervisory Authority's ("FINMA") categorization, where crypto-assets are divided into three main categories, based on their economic function: "payment tokens" that may serve as a means of exchange or payment for a product or a service, "investment/asset tokens" that may have profit-rights attached to it and "utility tokens" that may enable access to a specific product or service. A fourth category would be the "hybrid crypto-asset", reserved for those crypto-assets serving more than one of the previous economic purposes at the time or that might have its features altered throughout their lifecycle.

On that basis, the EC consultation, taking into account the considerations made by other EU institutions, categorized crypto-assets as "regulated" and "unregulated."

[10] *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN.*

[11] *Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1600960374694&uri=COM:2020:594:FIN.*

Chart 1. – Basic crypto-asset categorization combining the EC Consultation, the MiCA Regulation Proposal and the Pilot Regime Proposal



Note: this chart showcases the EC Consultation's conceptual framework to approach a classification of crypto-assets, completed with the MiCA and the Pilot Regime Regulation Proposals. Note, nevertheless, that this is not set in EU law.

A. REGULATED CRYPTO-ASSETS

Regulated crypto-assets are defined by the fact that they fall within the scope of the existing EU financial services regime. There are three types of regulated crypto-assets: "e-money crypto-assets", "Security tokens" and "DLT transferable securities".

According to the EC and other financial national authorities, regulated crypto-assets will normally encompass crypto-assets functioning as investment/asset tokens. In some cases, payment tokens, e.g. some "stablecoins", could also potentially fall under this category, as later explained. On the other hand, utility tokens will likely not meet the conditions to function as a Security or as e-money crypto-asset and will therefore normally be in the unregulated realm. For this reason, the MiCA Regulation Proposal includes utility tokens in its scope, as will be seen later.

E-money crypto-assets

The Electronic Money Directive ("EMD2")[13] sets out the rules for the business practices and supervision of e-money institutions. A crypto-asset will qualify as e-money (for the purposes of this paper, "e-money crypto-asset") to the extent that it satisfies each element of its legal definition in EMD2:

- Electronically stored monetary value.
- Represented by a claim on the issuer.
- Issued on receipt of funds for the purpose of making payment transactions to individuals or entities other than the e-money issuer.

From a practical perspective, the UK Financial Conduct Authority ("FCA") stated in its Guidance on Crypto-assets ("FCA Report") that payment tokens such as bitcoin, ether and others are unlikely to represent e-money because, amongst other things, they are not usually centrally-issued on the receipt of funds, nor do they represent a claim against an issuer.[14] Furthermore, the FCA considers that crypto-assets that establish a new sort of unit of account rather than representing fiat funds are unlikely to amount to e-money unless the value of the unit is pegged to a fiat currency.[15]

Very interestingly, the MiCA Regulation Proposal has included a specific definition for "e-money tokens" as opposed to e-money crypto-assets. We will explore this later, under section B.

Security tokens

The Markets in Financial Instruments Directive II ("MIFID2")[16] provides a list of instruments qualifying as "financial instruments" under its perimeter, including, inter alia, "transferable securities", "money market instruments", "units

in collective investment undertakings" and various derivative instruments. Depending on their specific features, crypto-assets could qualify as some of these instruments, especially as transferable securities. Following the EC Consultation's categorization, crypto-assets qualifying as transferable securities[17] or other financial instrument are referred to as "Security tokens".

A majority of the respondents in ESMA's survey to EU's national financial authorities agreed that the existence of attached profit rights (whether or not alongside ownership or governance rights) was sufficient for a crypto-asset to constitute a transferable security, provided the

---

[13] Electronic Money Directive (2009/110/EC).

[14] Financial Conduct Authority (FCA). (2019), Guidance on Cryptoassets, July version. Retrieved from: https://www.fca.org.uk/publication/consultation/cp19-03.pdf, p. 31.

[15] Ibid., p. 45.

[16] Markets in Financial Instruments Directive II (2014/65/EU).

[17] The term "transferable securities" is defined as those "classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as: (i) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;(ii)bonds or other forms of securitised debt, including depositary receipts in respect of such securities; and (iii) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures".

[18] European Securities and Markets Authority (ESMA). (2019), Advice Initial Coin Offerings and Crypto-Assets. Retrieved from https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p. 5.

crypto-asset was freely tradable and did not function as a payment instrument.[18]

Notably, ESMA excluded pure payment tokens (such as bitcoin, ether, and litecoin) from the survey on the basis that they are unlikely to qualify as "financial instruments". Likewise, national financial authorities showed consensus around the suitability of excluding pure utility-type crypto-assets from the perimeter of the existing financial regulation across EU member states on the basis that the rights they convey seem to be too far away from the financial and monetary structure of a transferable security and/or a financial instrument.[19]

The same line of though was followed by the Securities and Markets Stakeholders Group ("SMSG") in an advice to ESMA in October 2018.[20] The organization comes to the conclusion that payment tokens are not currently covered by MIFID2 nor other financial regulations. Nevertheless, the SMSG warns that transferable payment tokens are increasingly regarded as investment assets giving rise to similar risks to the capital markets (investor protection concerns and market abuse concerns) even proposing to bring these crypto-assets under the definition of financial instrument[21].

In the case of utility tokens, the SMSG is of the opinion that they have the potential to become investment objects only when they are transferable. On the contrary, where they can only be used in relation to the issuer they would not be under the scope of financial services regulations, unless they could qualify as e-money[22].

---

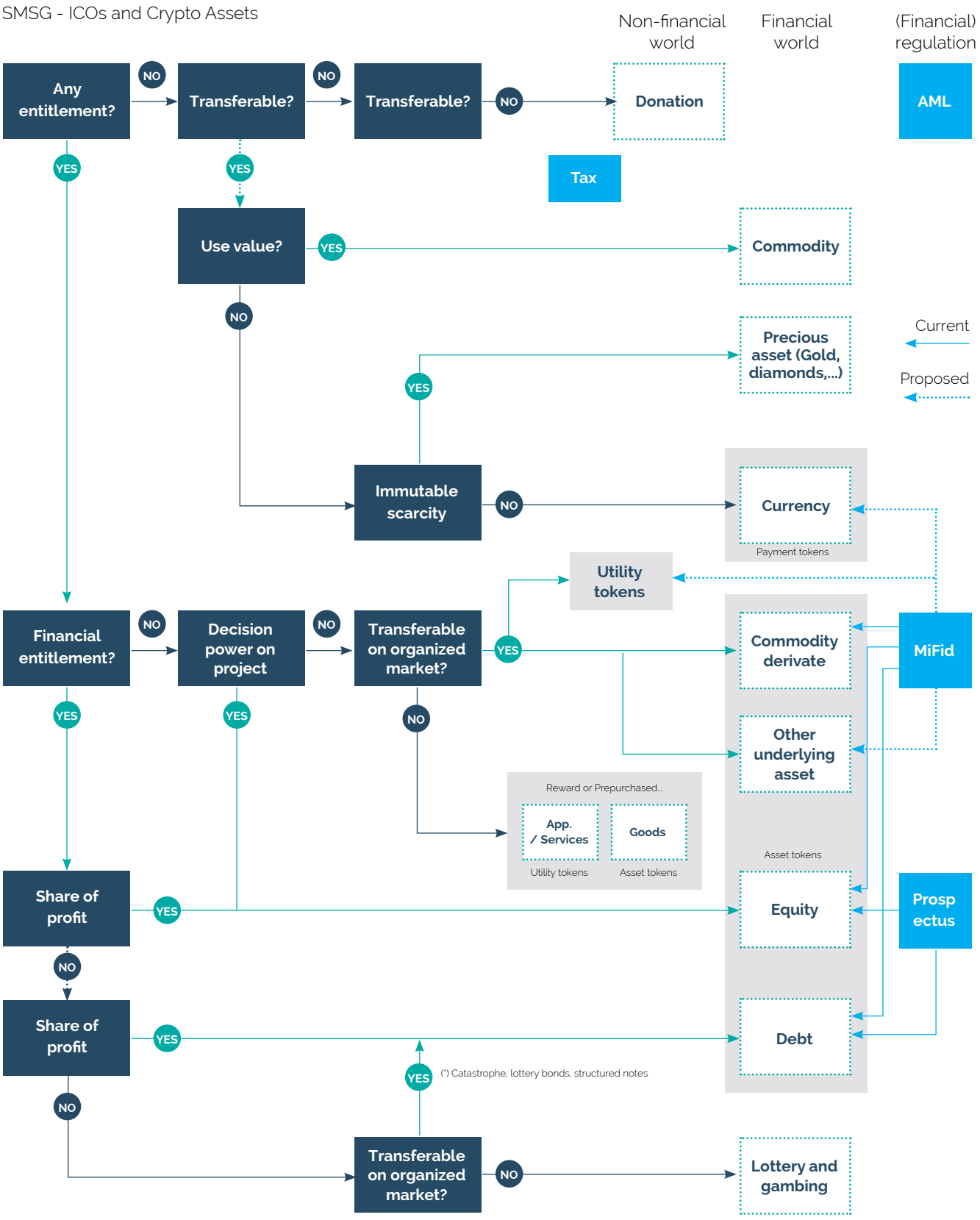
[19] *Idem, p. 20.*

[20] *Securities and Markets Stakeholder Group (SMSG). (2018), Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets. Retrieved from: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.*

[21] *Ibid., p. 13-14.*

[22] *Idem.*

Chart 2. – Applicability of financial services regulations to crypto-assets, according to the SMSG.



DLT Transferable Securities

The Pilot Regime Proposal, article 5, states that "DLT transferable securities" means transferable securities within the meaning of article 4(1)(44) (a) and (b) of MIFID2 that are issued, recorded, transferred and stored using a DLT.

DLT transferable securities are, therefore, a specific subset of Security tokens, which are limited to those matching the definition of transferable security under MIFID2. The Pilot Regime Proposal creates this token's category to limit the type of financial instruments that could be admitted to trading in "DLT market infrastructures"[23]. As we will explore below, only certain DLT transferable securities meeting some the conditions may be admitted to trading in these infrastructures.

B. CRIPTOACTIVOS NO REGULADOS

Unregulated crypto-assets are those falling outside the perimeter of the EU financial services regime. This category encompasses a wide variety of crypto-assets, normally utility and payment-type crypto-assets as well as crypto-assets with a hybrid function.

Note that the term unregulated does not mean that these crypto-assets are outside the scope of any EU legislation but merely that the financial services regulation framework does not apply to them. For instance, payment tokens will normally fall under the definition of "virtual currency" and thus subject to AML/CFT provisions[24]. Likewise, the sale of unregulated crypto-assets to a public qualifying as "consumers" will trigger the application of the EU package on consumer protection. Tax considerations are also a relevant legal angle when analysing the legal implications attached to the operation with crypto-assets.

Outside the scope of non-financial regulations (i.e. when crypto-assets do not qualify as financial instruments or as e-money), legislation specific to the DLT realm might be uphold in the future through the Regulation on MiCA. The EC's MiCA Regulation Proposal defines, among others, terms relevant to the development of a token taxonomy for the EU, including "crypto-asset", "utility token", "e-money token" and "asset-referenced token".

The definition of crypto-asset in this Regulation Proposal[25] is as wide as possible to capture all types of crypto-assets which currently fall outside the scope of EU financial services legislation to ensure that the Regulation is future-proof and keep pace with innovation and technology developments in the sector. Beyond the general definition of crypto-assets, the MiCA Regulation Proposal distinguishes between three sub-categories of crypto-assets that are be subject to specific requirements: utility tokens, e-money tokens and asset-referenced tokens.

Utility tokens

According to the MiCA Regulation Proposal, utility tokens refers to "a type of crypto-assets which are intended to provide access digitally to an application, services or resources available on a distributed ledger and that are accepted only by the issuer of that token to grant access to such application, services or resources available".

The fact that the MiCA Regulation Proposal decided to define this kind of asset as a specific sub-category and leave payment tokens undefined could be a good indicator to show that this Regulation excludes pure payment tokens from its scope. That would be the case if payment tokens do not qualify as e-money tokens or asset-referenced tokens. This entails that crypto-assets such as bitcoin, litecoin, bitcoin cash or other projects which are not focused on stabilising the token's value, are out of the scope of this Regulation Proposal.

---

[23] Article 2(2) of the Pilot Regime Proposal defines a DLT market infrastructure means either a "DLT multilateral trading facility" or a "DLT securities settlement system", as defined in articles 2(3) and (4) of the same Regulation.

[24] 5th Anti-Money Laundering Directive (Directive 2018/843/EU).

[25] Crypto-asset is defined in the MiCA Regulation Proposal, article 3(1)(b), as "a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology".

E-money tokens

According to the MiCA Regulation Proposal, an e-money token is a "type of crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by being denominated in (units of) a fiat currency". [26] The Regulation Proposal determines that crypto-assets qualifying as e-money under EMD2 but not as e-money tokens under the MiCA Regulation Proposal, will be outside MiCA's perimeter.

Despite their similarities, some differences exist between e-money under EMD2 and e-money tokens. For instance, holders of e-money under EMD2 are always provided with a claim against an e-money institution and have a contractual right to redeem their e-money against fiat currency at par value with the fiat currency and at any moment. By contrast, some e-money tokens do not provide their holders with such a claim on their issuers and could fall outside the scope of EMD2. In addition, other e-money tokens do not provide a claim at par with the fiat currency they are referencing or limit the redemption period.

The reason to create the legal institution of e-money tokens as opposed to crypto-assets falling under the scope of EMD2 (e-money crypto-assets), is to create a wide definition to capture all the types of crypto-assets referencing one single fiat currency on the crypto-asset market that prevents regulatory arbitrage with the provisions of the EMD2 or the circumvention of EU rules.[27]

Asset-referenced tokens

Asset-referenced token means a "type of crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of several fiat currencies, one or several commodities or one or several crypto-assets, or a combination of such assets".

---

[26] See article 3(1)(d) of the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN.

[27] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN, p. 16-17.

From the last two definitions, it is clear that the MiCA Regulation Proposal has its eye focused on stablecoins. Nevertheless, relevant complexities remain when trying to fit stablecoins in existing legal institutions, including all the above mentioned (financial instruments, an e-money crypto-asset, an e-money token or an asset-referenced token).

For instance, in its response to the EC Consultation, the European Association of Cooperative Banks responded that "it is absolutely unclear what they are for the time being", potentially being from just a "marketing label", "e-money" or some kind of tokenised money market fund with assets kept at a custodian/depositary.[28]

Other stakeholders have stated that crypto-assets with commodities as underlying assets share the same characteristics as commodity derivatives, for instance, the SMSG.[29] ESMA categorised stablecoins as similar to securities with reference to transferable commodities, and, therefore, potentially part of the definition of "transferrable securities" under MIFID2.[30] Further, in October 2019, the G7 published a paper on stablecoins[31] which seems to follow a similar approach to ESMA.

III. REGULATED CRYPTO-ASSETS: AMENDMENTS TO THE EU FINANCIAL SERVICES LEGAL FRAMEWORK TO BE EFFECTIVELY APPLIED TO CRYPTO-ASSETS

Despite the EU financial legislation was not drafted with crypto-assets in mind, several existing legal institutions, such as e-money or transferable securities, can serve today to bring some crypto-assets to EU legal grounds.

However, the application of the EU legislation to the field of crypto-assets is not exempt for difficulties. At a starting point, there is the obvious difficulty of subsuming brand new, innovative creations in already established legal institutions that were not developed with them in mind. In addition, some current provisions may directly inhibit the possibility of using DLT. Finally, some crucial aspects are not harmonized at EU level and some EU member states are taking different approaches to similar cases, thus resulting in lack of uniformity which can eventually give rise to regulatory arbitrage.

The EC Consultation explored these difficulties and sought views to alleviate them.

This section goes over two of the main difficulties to apply the existing financial services regulatory framework to crypto-assets and concludes with the possible regulatory action foreseen by the EC to deal with it.

A. Unclear application of the regulatory framework and legal uncertainty

When crypto-assets are considered to fall inside the EU financial regulatory perimeter, it is not always easy to determine how the existing framework should be applied. These circumstances are challenging for all actors involved (including financial supervisors, crypto investment firms and crypto investors) and leads to legal uncertainty. For instance, investors can have difficulties in determining whether they are entitled to legal protection and many market participants are wondering which rules they should adhere to, if any, to make sure that the activities they conduct are legally compliant.

This is especially clear when the novelty posed by crypto-assets challenges the current framework's ability to serve as a one-size-fits-all solution. Clear examples of this can be stablecoins, hybrid platforms, hybrid crypto-assets and decentralized exchanges.

---

[28] See p. 58 in EACB's response to the EC Consultation in the link provided in footnote 46.

[29] Securities and Markets Stakeholder Group (SMSG). (2018), Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets. Retrieved from: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf, p. 11.

[30] European Securities and Markets Authority (ESMA). (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.19.

[31] G7 Working Group on Stablecoins. (2019), Investigating the impact of global stablecoins. Retrieved from: https://www.bis.org/cpmi/publ/d187.pdf.

B. Regulatory fragmentation and arbitrage

Where crypto-assets qualify as transferable securities or other types of financial instruments under MIFID2, a comprehensive set of EU financial rules, including the Prospectus Regulation ("PR")[32], the Transparency Directive, MIFID2, the Market Abuse Directive, the Short Selling Regulation and others are likely to apply to their issuer and/or firms providing investment services/activities to those instruments.[33] Activities concerning Security tokens would qualify as investment services/activities and transactions in Security tokens admitted to trading or traded on a trading venue would be captured by various financial provisions.[34]

Despite the common framework established by MIFID2, the actual classification of a crypto-asset as a financial instrument is the responsibility of the financial authorities in each member state and will depend on the specific national implementation of EU law based on the information and evidence provided to that EU national financial authority.[35] For instance, the definition of financial instruments has been differently transposed in EU member states (i.e. some employ a restrictive list to define transferable securities, others use broader interpretations). As a result, EU member states might reach different conclusions when assessing the legal classification of a given crypto-asset as a Security token, posing new challenges to adopting a common regulatory and supervisory framework across the EU. Furthermore, the current situation challenges the capacity of financial authorities to interpret the regulatory framework consistently, which increases the risk of regulatory arbitrage.

For instance, Germany has amended its Banking Act to implement AMLD5 in the country and has considered crypto-assets with payment purposes to be financial instruments if they fall under the following definition:

- A digital representation of value which;
- has neither been issued nor guaranteed by a central bank or public body;
- it does not have the legal status of currency or money but;
- on the basis of an agreement or actual practice;
  - is accepted by natural or legal persons;
  - as a means of exchange or payment; or
  - serves investment purposes; and
- it can be transferred, stored and traded by electronic means.

The German Banking Act excludes from this definition those crypto-assets legally functioning as e-money as well as certain monetary assets.[36]

Another example can be the Netherlands where crypto-assets are considered a security by the national competent financial authority if they are transferable and negotiable on the financial markets; and represent either (i) a share or equivalent right or instrument; (ii) a bond or other debt instrument; or (iii) any other instrument that can be converted into a share, bond or equivalent or that can be settled in cash. The definition of security under Dutch law lists the three categories above as a closed, exhaustive list, in contrast to the MIFID2 definition which uses a non-exhaustive list which remains open to other type of securities. As a result, the Dutch financial authority's ability to interpret the term is significantly restricted in comparison to other member states in the EU.[37]

C. Possible regulatory action

In the May version of the non-paper, the EC explored the possibility to tackle the above-

[32] Prospectus Regulation (2017/1129/EU).

[33] European Securities and Markets Authority (ESMA). (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[34] European Commission (EC). (2019), Consultation Document on an EU framework for markets in crypto-assets. Retrieved from https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf, p. 29.

[35] European Securities and Markets Authority (ESMA). (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[36] Federal Financial Supervisory Authority (BAFIN). (2020), Guidance Notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG). Retrieved from: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html.

[37] Authority for the Financial Markets (AFM), De Nederlandsche Bank (DNB). (2018), Cryptos – Recommendations for a regulatory framework. Retrieved from https://www.dnb.nl/en/binaries/AFM-DNB%20Crypto%20Recommendations_tcm47-381603.pdf.

mentioned problems through a combination of legislative and non-legislative measures.[38] In particular, the EC indicated three options to consider:

- Non-legislative measures which would provide guidance on how existing legislation applies to crypto assets;
- targeted legislative changes removing provisions acting as a barrier to issuance, trading and post-trading of Security tokens; or
- a pilot regime for DLT market infrastructures for crypto-assets that qualify as financial instruments.

C1. Guidance on how existing legislation applies to crypto assets

The non-paper proposed an interpretative communication where the EC sets its view on the characteristics crypto-assets should have to qualify as financial instruments or e-money under the EU financial services regulatory framework. As an additional action, the non-paper mentioned that the EC could provide guidance on how existing sectoral legislation applies, according to the EC, to crypto-assets that would qualify as "financial instruments" (such as MIFID2, the Prospectus Regulation, the Central Security Depositary Regulation and the Settlement Finality Directive).[39]

C2. Potential targeted amendments to existing financial services legislation

Where provisions of sectoral legislation would clearly hinder or prevent the use of DLT or Security tokens or where proper application of the legislation in a DLT environment cannot be assured, the EC may present targeted amendments to address these issues. These amendments might not require Level 1 changes, but instead could require level 2 modifications and could also be done if and when the legislation in question is being reviewed.[40]

Those targeted changes would enable the use of centralised networks and permission-based DLT. Most notably, this initiative could include a targeted amendment to the notion of financial instruments under the MIFID2, to make sure that such an instrument can be issued on a DLT.[41]

This initiative could include a targeted amendment to the notion of financial instruments under the MIFID2, to make sure that such an instrument can be issued on a DLT

In addition, the Pilot Regime Proposal indicates that the EC is planning to release a Directive amending several financial regulations,[42] including MIFID2, to allow "DLT MTFs"[43] to be able to request an exemption from the obligation of intermediation (i.e. admit as members or participants only investment firms, credit institutions and other persons who have sufficient level of trading ability), thus being able to onboard retail investors directly. In this regard, by contrast to traditional MTFs, many trading platforms for crypto-assets offer a disintermediated access and provide direct access to retail clients.

---

[38] European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Retrieved from https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf, p.4.

[39] Ibid.

[40] Ibid.

[41] European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Retrieved from https://drive.google.com/file/d/1ZBl_YSUcKblJCrsOtoQk66z4jtd7Dvkj/view, p.1.

[42] See, for instance, recital 17 of the Pilot Regime Proposal.

[43] According to article 2(3) of the Pilot Regime Proposal, a "DLT MTF" means a multilateral trading facility (as defined in article 4(1)(22) MIFID2), operated by an investment firm or a market operator, that only admits to trading DLT transferable securities and that may be permitted, on the basis of transparent, non-discretionary, uniform rules and procedures, to: (a) ensure the initial recording of DLT transferable securities; (b) settle transactions in DLT transferable securities against

C3. Proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology

In July's version of the non-paper, the EC noted that there is a lack of market infrastructure in the DLT realm as legal uncertainty discourages the establishment of trading venues or central security depositories ("CSDs") . This infrastructure would enable the trading and settlement of crypto-assets, would allow the development of secondary markets for Security tokens to support the nascent primary market and would help to create the conditions for these markets to scale.

To solve this issue, the EC has released the Pilot Regime Proposal, as part of their proposal for an EU framework on crypto-assets.

The pilot regime would function as a temporary sandbox open for a period of up to six years, during which DLT market infrastructures can operate exempted from some specific requirements under the UE financial services legislation. The aim is to temporarily remove certain regulatory obstacles that could be preventing the development of DLT infrastructure, therefore enabling both market participants and regulators to gain experience and to explore the risks posed by this infrastructure.

A DLT market infrastructure would either function as a DLT MTF or a DLT CSD. Operators of these venues would be required to obtain an authorization by their local financial authority, on top of their existing authorisation as investment firm, market operator (in the case of DLT MTFs) or as a central security depository (in the case of DLT CSDs).

During the time-limited experimentation, the DLT market infrastructure would only be allowed to admit to trading or to record on the ledger simple financial instruments (i.e. shares and bonds) that are not liquid. In turn, the participants can apply for exemptions when operating, most notably the possibility to admit retail investors in their customer base, thus removing the obligation of intermediation through investment firms, credit institutions and other persons with sufficient level of trading ability.

National financial authorities would have the power to impose corrective measures on the DLT market infrastructure and to withdraw the permission under some circumstances. ESMA would fulfil a coordination role between competent authorities.

National financial authorities would have the power to impose corrective measures on the DLT market infrastructure and to withdraw the permission under some circumstances.

The Proposal estates that, after a five-year period from the entry into application of this Regulation, ESMA should report to the EC on this pilot regime for DLT market infrastructures, including on the potential benefits linked to the use of DLT, the risks raised and the technical difficulties. Based on ESMA's report, the EC should report to the Council and European Parliament. This report should assess the costs and benefits of extending this regime on DLT market infrastructures for another period of time, extending this regime to new type of financial instruments, making this regime permanent with or without modifications, bringing modifications to the EU financial services legislation or terminating this regime.

---

[42] Consúltese, por ejemplo, el considerando 17 del Reglamento de Régimen Piloto.

[43] De acuerdo con el artículo 2.3 de la Propuesta de Régimen Piloto, un "SMN DLT" significa un sistema multilateral de negociación (según se define en el artículo 4.1.22) MIFID2), operado por una entidad de servicios de inversión o un operador de mercado, que solo admite a negociación valores negociables sobre DLT.

[44] Un depositario central de valores es persona jurídica que gestione un sistema de liquidación de valores, de conformidad con el reglamento 909/2014.

IV. UNREGULATED CRYPTO-ASSETS: A BESPOKE REGIME

A. Introduction

The ESMA Report raised concerns regarding the risk of consumer/investor lack of protection given that most crypto-assets are not likely to qualify as financial instruments under MIFID2 and, therefore, are likely to fall outside the existing EU financial services rules . As a result, consumers and investors will not benefit from the safeguards provided by these rules while not being able to easily distinguish whether crypto-assets available in the same trading venues are within the scope of the EU's financial legal framework. In addition, some EU member states have implemented or are considering bespoke regimes for crypto-assets that do not qualify as financial instruments, with the notable example of the French PACTE law and Malta´s three acts on DLTs, thus helping to foster regulatory fragmentation across the EU.

With that in mind, the EC Consultation also sought views to assess whether regulating the unregulated crypto-asset space could be beneficial at this point. As a result, the MiCA Regulation Proposal proposes a bespoke regime to regulate unregulated crypto-assets.

B. Proposal for a regulation on Markets in Crypto-Assets Regulation

The EC has developed a regulation to establish harmonised requirements at EU level for issuers that seek to offer their crypto-assets across the EU and crypto-asset service providers wishing to apply for an authorisation to render their services in the single market, where these crypto-assets do not qualify as financial instruments. This initiative would replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation.

B1. Requirements on issuers

In relation to the issuance of crypto-assets, MiCA establishes requirements on issuers of:

- crypto-assets (tokens outside the definition of a financial instrument, with utility tokens in mind);
- asset-referenced or significant asset-referenced tokens; and
- e-money tokens.

In relation to the issuance of crypto-assets, the MiCA Regulation Proposal mandates the publication of a harmonised whitepaper/information document with mandatory disclosures (detailed description of the issuer, the project and planned used of funds, conditions of the offer, rights and obligations attached to the crypto-assets and risks). Small offerings (value under EUR 1 million within a twelve-month period) and offerings aimed at qualified investors as defined in the PR might be exempted from this requirement, as well as other cases listed in article 4(2) of the Proposal. This document shall not be sanctioned by member states' financial authorities although it should be notified prior to its publication.

It will be the responsibility of the issuer to justify before member states' financial authorities why the crypto-asset in question does not qualify as a financial instrument or as a deposit under MIFID2 or as e-money under EMD2.

---

[45] Autoridad Europea de Valores y Mercados. (2019). Advice Initial Coin Offerings and Crypto-Assets. Accedido desde https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, p.5.

[46] En Francia, la ley PACTE, por sus siglas en francés, ha creado un marco específico para la oferta de tokens de utilidad al público y para regular ciertos aspectos, como los riesgos operativos y de seguridad, los mecanismos de control interno, la resiliencia de los sistemas informáticos o el conflicto de intereses, para diferentes proveedores de servicios sobre criptoactivos, en aquellos casos en los que los criptoactivos no encajan en la definición de instrumento financiero de MIFID2. El régimen es opcional, lo que significa que los prestadores de servicios no tendrán que cumplir con sus normas y requisitos a menos que decidan opten por someterse a él, punto a partir del cual deberán cumplir en su totalidad. En otras palabras, esta configuración legal ofrece a los proveedores de servicios sobre criptoactivos ganar en seguridad jurídica a cambio de asumir ciertos costes para el cumplimiento regulatorio. Este enfoque novedoso ha sido alabado y criticado, siendo la voz más destacada entre las críticas la de AEVM, que aunque comprende la intención de apoyar estos instrumentos, destaca que este tipo de iniciativas no ayudan a proporcionar un marco homogéneo en toda la UE.

En Malta, el legislador ha adoptado tres leyes relacionadas con DLT, que entraron en vigor el 1 de noviembre de 2018: (i) la Ley de Activos Financieros Virtuales, (ii) la Ley de la Autoridad de Innovación Digital de Malta, y (iii) el Acuerdo de Tecnología Innovadora y Ley de Servicios. Estas tres leyes introducen, entre otras medidas, un requisito para que los emisores de activos financieros virtuales elaboren y pongan a disposición un whitepaper, requisitos de licencia para proveedores de servicios financieros virtuales como corredores, reglas de conducta comercial para titulares de licencias y ciertos requisitos sobre blanqueo de capitales para titulares de licencias.

It will be the responsibility of the issuer to justify before member states' financial authorities why the crypto-asset in question does not qualify as a financial instrument

Issuers of asset-referenced tokens will have to obtain authorization before conducting an offering unless the average standing amount of asset-referenced tokens does not exceed EUR 5,000,000 over a period of 12 months or the offer is addressed at qualified investors only. Issuers of these tokens will also have to comply with a number of requirements, for instance to be established as an EU legal entity, to disclose the rights attached to the asset-referenced token, including any potential direct claim on the issuer or the reserve of assets, and be required to publish a whitepaper with additional mandatory disclosures to those mandated in the case of regular issuances. Further, the whitepaper will be have to be approved by national financial authorities (unless the offer did not need to be subject to authorization, in which case the whitepaper would only need to be notified), which will be in charge of the authorisation and ongoing supervision of issuers of asset-referenced tokens.

As for the issuers of e-money tokens, the MiCA Regulation Proposal imposes the obligation for these e-money tokens to be issued either by a credit institution authorised under Regulation (EU) 2013/575 or by an electronic money institution under EMD2. It is worth noting that they shall grant their users with a claim at any moment and at par value with the fiat currency referenced.

B2. Service providers subject to authorization

In relation to crypto-asset service providers, the MiCA Regulation Proposal would regulate the following services:

- Custody and administration of crypto-assets on behalf of third parties;
- operation of a trading platform for crypto-assets;
- exchange of crypto-assets for fiat currency;
- exchange of crypto-assets for other crypto-assets;
- reception and transmission of orders for crypto-assets on behalf of third parties;
- execution of orders for crypto-assets on behalf of third parties;
- placing of crypto-assets;
- advice on crypto-assets; and
- payment transactions in asset-referenced tokens.

National financial authorities are envisaged to be in charge of the authorisation of the crypto-asset service providers. Once authorised, they would be allowed to provide their services across the Union.

IV. CONCLUSION

As discussed throughout this paper, there are several reasons to justify that legislative and non-legislative action is put in place to ensure that crypto-assets are adequately fit in the existing financial services regulatory framework and to regulate the risks derived from the lack of regulation in the case of unregulated crypto-assets.

The EC has put on the table a number of interesting proposals to go forward, entailing a package of legislative and non-legislative measures.

In relation to a crypto-asset taxonomy, some important definitions could accrue to the EU legal acquis through the MiCA Regulation, if enacted. In addition, a taxonomy of crypto-assets in the EU could be supported by non-legislative measures, for instance through guidelines by the EC or the EU authorities for financial supervision, to ensure a consistent interpretation of DLT terms across the EU.

In order to ensure that the existing EU financial regulatory framework can be effectively applied to crypto-assets, the EC proposes a combination of legislative and non-legislative measures:

- Non-legislative measures which would provide guidance on how existing legislation applies to crypto assets;
- targeted legislative changes removing provisions acting as a barrier to issuance, trading and post-trading of Security tokens; or
- a pilot regime for DLT market infrastructures for crypto-assets that qualify as financial instruments.

Finally, the EC has envisaged a bespoke legal regime for unregulated crypto-assets, the MiCA regulation, that could serve to alleviate the issues derived from the issuance of and operation with these crypto-assets.

Abbreviations:

AMLD5 – 5th Anti-Money Laundering Directive (Directive 2018/843/EU)
AML/CFT – Anti-money laundering and combatting the financing of terrorism
CSD – Central Securities Depositary
EACB – European Association of Cooperative Banks
EBA – European Banking Authority
EBA Report – Report with advice for the European Commission on crypto-assets
EC – European Commission
EC Consultation – Consultation Document on an EU framework for markets in crypto-assets
EMD2 – Electronic Money Directive (2009/110/EC)
ESMA – European Securities and Markets Authority
ESMA Report – Advice Initial Coin Offerings and Crypto-Assets
EU – European Union
DLT – Distributed Ledger Technology
FCA – Financial Conduct Authority
FCA Report – Guidance on Cryptoassets
MiCA - Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets.
MIFID2 – Markets in Financial Instruments Directive II (2014/65/EU)
MTF – Multilateral Trading Facility
PR – Prospectus Regulation
PSD2 – Payment Services Directive

Abuso de posición de dominio en plataformas digitales y blockchain

¿Vale el mismo collar para perros tan distintos?

Pablo Solano Díaz. Abogado. Uría Menéndez
(Todas las opiniones expresadas son estrictamente personales)

Los expertos en defensa de la competencia han vertido ríos de tinta sobre las características propias de las llamadas "plataformas digitales" en los últimos años. A modo de resumen, las plataformas multilaterales (es decir, las que hacen de intermediarios entre grupos de usuarios con demanda distinta, pero interrelacionada) ya existían en el mundo analógico (piénsese en las tarjetas de crédito, la prensa o la televisión). Sin embargo, en entornos digitales alcanzan un potencial inédito por (i) la fácil internalización de externalidades positivas producidas en un lado de la plataforma por un grupo de usuarios mediante su venta en el otro lado (por ejemplo, Google monetiza fácilmente la atención de los usuarios de servicios de búsqueda general vendiendo espacio publicitario a anunciantes); (ii) los reducidos costes de transacción, que aumentan aún más la capacidad de canalizar externalidades positivas entre lados de la plataforma (los denominados efectos indirectos efectos de red); (iii) la intensidad exacerbada de los rendimientos crecientes de escala debida a los mínimos costes marginales; o (iv) el mayor valor de los datos gracias a los avances tecnológicos de almacenamiento y análisis.

Estos rasgos hacen aplicables a las plataformas digitales (i) la ley de Coase, conforme a la cual,

ante escasos costes de transacción y con independencia de la asignación inicial de los recursos (o de la concentración de poder de mercado), las partes afectadas por externalidades alcanzan mediante la negociación un resultado eficiente en términos de Pareto; y (ii) la ley de Metcalfe, conforme a la cual las redes de comunicaciones presentan unos rendimientos crecientes de escala que hacen aumentar su valor a razón del cuadrado de su número de usuarios conectados a la red. El corolario es la tendencia natural de los mercados digitales a posiciones monopolísticas que maximicen las externalidades positivas producidas en la forma de efectos de red y que a menudo desbordan los mercados concretos y dan lugar a economías de gama.

Surgen así operadores de plataformas (los llamados gatekeepers) con un control cuasi regulatorio sobre puntos de entrada importantes o incluso esenciales (cuellos de botella) a grupos de mercados relacionados, que, en caso de captura de usuarios, forman ecosistemas cerrados (como podría ser iOS). Ello no tiene por qué plantear problemas de competencia si los cuellos de botella están libres de barreras permanentes y significativas a la entrada (como pueden ser la interoperabilidad imperfecta, la ausencia de multi-homing, la dificultad de portabilidad o el efecto de marca), en cuyo caso los efectos de red favorecerían la expansión rápida de nuevos entrantes. En cambio, de existir tales barreras, los efectos de red podrían reforzar la posición de los gatekeepers y colocarlos en posición tanto de falsear la competencia con otras plataformas por hacerse con los usuarios (la competencia por el mercado) como de favorecer artificialmente a su propio negocio en la plataforma (la competencia en el mercado).

Las premisas de funcionamiento de las redes blockchain son bastante distintas: (i) descentralización de la validación y el registro de operaciones en todos los nodos conectados; (ii) transparencia en cuanto a las operaciones realizadas y opacidad de su contenido, gracias a la criptografía; (iii) automaticidad del protocolo en el que se basa su funcionamiento; (iv) inmutabilidad de las operaciones ya registradas en bloques; y (v) estructura multi-capa formada por un nivel de plataforma en el que se escribe el protocolo y un nivel de aplicaciones que funcionan sobre la base de ese protocolo. Ello supone que la blockchain se rija por leyes económicas diferentes a las propias de las plataformas digitales clásicas. En primer lugar, a diferencia de las plataformas como Facebook o Google, las redes blockchain no son intermediarios que canalizan externalidades ente grupos de usuarios. De hecho, su razón de ser es precisamente la eliminación de la intermediación al permitir a los usuarios aprovechar directamente los efectos de red entre ellos. De este modo, el único plano en el que en realidad habría propiamente competencia es dentro de la red y no entre redes. Es decir, a diferencia de las plataformas digitales, en la blockchain solo habría competencia en el mercado y no por el mercado.

> La razón de ser de las redes blockchain es la eliminación de la intermediación al permitir a los usuarios aprovechar directamente los efectos de red entre ellos

Ello no solo afecta al tipo de conductas que pueden considerarse abusivas (al no haber competencia por el mercado tampoco podría falsearse), sino también a la definición del mercado de referencia en el que se analiza la posición de dominio. Así, no tendría tanto sentido delimitar un mercado de la tecnología blockchain en el que compitieran las distintas redes como definir un mercado separado por red o, como propugna la doctrina clásica, por cada grupo de usuarios con demanda diferenciada (por ejemplo, distintos mercados por tipos de aplicaciones instaladas sobre la plataforma). Otra opción sería definir solo los mercados de bienes y servicios analógicos subyacentes, siendo la blockchain únicamente analizada

como ventaja competitiva en la comercialización de estos bienes y servicios, que es como se trata a los datos bajo el marco analítico actual de competencia.

En segundo lugar, la difusión del poder entre nodos y el carácter colaborativo de la blockchain, que desafía la propia concepción de la competencia en una economía de mercado como un juego no cooperativo, dificultan hablar de posición de dominio. Por un lado, parece que las características de una red blockchain no encajan con las de una empresa ni con las de una asociación de empresas, sino que habría que identificar un grupo de usuarios con intereses e influencia cualificados para afirmar su dominancia dentro de la red (como postula la teoría de la granularidad).

Por otro lado, en los protocolos de blockchain más extendidos, se retribuye a los nodos validadores con tokens para incentivar la validación sin generar inflación en las comisiones cobradas a los usuarios por realizar operaciones en la red. En las redes blockchain en las que la selección del nodo validador es aleatoria (como Bitcoin), los incentivos de los usuarios para participar como nodos se reducen conforme aumenta su número, pues que haya más nodos supone una menor probabilidad de ser aleatoriamente seleccionado para validar y obtener tokens. Este fenómeno, denominado efecto token, es inverso a la ley de Metcalfe que rige en las plataformas digitales. Así, a diferencia de las plataformas digitales, la blockchain presenta rendimientos decrecientes de escala, por lo que su capacidad de monopolización es menor y se reduce conforme la red crece.

A la luz de las limitaciones del análisis del abuso de posición de dominio en redes blockchain, cabe esperar que las teorías del daño sigan ancladas en restricciones que afecten a plataformas digitales clásicas, cuando no a mercados puramente analógicos. Tomando como ejemplo el proyecto Libra promovido por Facebook, el debate teórico sobre posibles abusos apunta a la posibilidad de combinar cuentas de usuarios de Facebook y WhatsApp con el monedero de tokens de Libra (Calibra), formándose así un cuello de botella que lleve a definir un hipotético mercado adyacente de monederos compatibles con Libra del que puedan verse excluidos los rivales de Calibra. Otras posibles teorías del daño (también reconducibles a categorías ya conocidas) serían la utilización de las normas de gobernanza de la red para excluir a operadores no miembros del consorcio desarrollador, el cobro de comisiones excesivas o predatorias o incluso un abuso de combinación de datos de usuarios de Libra, Facebook y WhatsApp sin consentimiento expreso al estilo de la investigación de la Bundeskartellamt en relación con Facebook.

REFERENCIAS:

Catalini, C., Gans, J. S. (2016), Some simple economics of the blockchain, Working Paper 22952, National Bureau of Economic Research.

Crémer, J., De Montjoye, Y.-A., Schweitzer, H. (2019), Competition policy for the digital era, Oficina de publicaciones de la Unión Europea.

Evans, D. S. (2008), Competition and Regulatory Policy for Multi-sided Platforms with Applications to the Web Economy, 2 Concurrences, 57-62.

Lianos, I. (2018), Blockchain competition, Centre for Law, Economics and Society Research Paper Series 4/2018, University College London.

Massarotto, G. (2020), Antitrust in the blockchain era, Notre Dame Journal of Emerging Technologies, 252-278.

Organización para la Cooperación y el Desarrollo Económicos (2018), Blockchain Technology and Competition Policy, Documento de la Secretaría, Dirección de asuntos financieros y empresariales Comité de competencia, abril.

Schrepel, T. (2020), Libra: A Concentrate of "Blockchain Antitrust", 118 Michigan Law Review, 160-169.

Schrepel, T. (2020), The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems, 50 Pages, Harvard University (Berkman Center), Utrecht University School of Law, University Paris 1 Panthéon-Sorbonne, enero.

Schrepel, T., Buterin, V. (2020), Blockchain code as antitrust.

Solano, P. (2017), EU Competition Law needs to install a plug-in, 40(3) World Competition, 393–420.

Abuse of dominance in digital platforms and blockchain

Is the same bottle good for so different wines?

Pablo Solano Díaz. Lawyer. Uría Menéndez
(All opinions expressed are strictly personal)

The features of so-called "digital platforms" have grabbed the headlines of competition law specialised publications for the last years. To sum up the question, multi-sided platforms (i.e. those operating as interface between groups of users presenting different but interrelated demand) already existed in the analogue world (think of credit cards, press or television). However, they deploy an unheard-of potential in the digital environment due to (i) easy internalisation of positive externalities generated by a user group on one side of the platform though their selling to a group on the other side (e.g. Google monetises easily general search users' attention by selling advertising space to advertisers); (ii) reduced transaction costs – which further increase the ability to channel positive externalities between platform sides (i.e. so-called indirect network effects); (iii) the exacerbated intensity of increasing returns to scale because of minimal marginal costs; or (iv) the greater value of data thanks to developments in storing and analysis technology.

These characteristics make applicable to digital platforms (i) the Coase theorem – whereby, in the presence of limited transaction costs and regardless of the initial allocation of resources

(or the concentration of market power), those parties affected by externalities will reach a Pareto-efficient outcome though bargaining; and (ii) Metcalfe's law – whereby communication networks feature increasing network effects that make their value rise proportionally to the square of the number of connected users. The corollary is a natural tendency of digital markets toward monopolistic positions that maximise positive externalities arising in the form of network effects, and often spilling over into neighbouring markets and producing economies of scope.

This is the setting where gatekeepers emerge. Gatekeepers are platform operators having a quasi regulatory control over important, or even essential, entry points (i.e. bottlenecks) to arrays of related markets – which, in case of user lock-up, may form closed ecosystems (as may be iOS). This does not have to pose any concerns from the competition point of view where bottlenecks are free from permanent and significant barriers to entry (such as imperfect interoperability, lack of multi-homing, difficult portability, or brand effect) – in which case network effects would catalyse new entrants' swift expansion. Conversely, if those barriers did exist, network effects could reinforce gatekeepers' footholds and place them on a position both to distort competition with other platforms over users (competition for the market) and to artificially favour their business on the platform itself (competition in the market).

The functioning of blockchain networks is based on quite different principles: (i) decentralisation of validation and recording of transactions in all connected nodes; (ii) transparency as regards executed transactions and opacity as regards their content thanks to encryption; (iii) automaticity of the protocol underpinning its functioning; (iv) immutability of already block-recorded transactions; and (v) multi-layer structure made of a platform layer where the protocol is scripted and an application level where software runs on the basis of such protocol. This means that blockchain is governed by different economic laws from classic digital platforms.

Firstly, unlike platforms like Facebook and Google, blockchain networks are not intermediaries channelling externalities between user groups. As a matter of fact, their very raison d'être is precisely the removal of intermediation by allowing users to directly reap network effects arising among them. Therefore, there would only be competition within the network but not among networks. That is, unlike in digital platforms, there would only be competition in the market, not quite for the market.

Not only does this affect the sort of practices that may be considered abusive (since there is no competition for the market to be distorted) but it also has an impact on the definition of the relevant market within which dominance is to be appraised. From this perspective, defining a market for blockchain technology would not make so much sense as delimiting

The rationale behind blockchain networks is the elimination of intermediation by allowing users to directly take advantage of the network effects of each other

separate markets by network, or, following the traditional doctrine, by user group having distinct demand (e.g. different markets by type of application running on the platform). An alternative would be defining markets only for the underlying analogue goods and services, while blockchain is only analysed as a competitive advantage in the marketing of such goods and services – just as data are treated under the current competition analytical framework.

Secondly, the power diffusion among nodes and the collaborative nature of blockchain, which calls into question the very construc-

tion of competition in market economy as a non-cooperative game, make it difficult to talk about dominance. On the one hand, the features of blockchain networks seem to sit ill at ease with the concept of undertaking or even associations of undertakings, but require the identification of a user group with qualified interests and influence in order to assert their dominance within the network (as proposed by the theory of granularity).

On the other hand, under more widespread blockchain protocols, validating nodes are rewarded with tokens in order to incentivise validation without generating inflation in commissions payed by users for running transactions on the network. In blockchain networks where the choice of validating nodes is random (e.g. Bitcoin), incentives for users to participate as nodes decrease as the numbers of users increase, because more nodes means littler likelihood of being randomly chosen to validate and receive tokens. This phenomenon, known as token effect, is the converse of Metcalfe's law governing digital platforms. Consequently, unlike digital platforms, blockchain networks feature decreasing returns to scale, thereby their monopolisation potential being smaller and declining as the network grows.

In light of the limitations to the assessment of abuse of dominance in blockchain networks, one may expect that theories of harm remain anchored in restrictions affecting classic digital platforms, if not purely analogue markets. Taking Facebook-backed Libra project as an example, the theoretical debate over potential abuses points toward the possibility to combine Facebook and WhatsApp user accounts with Libra's token wallet (Calibra) – so that a bottleneck arises allowing for the definition of a hypothetical adjacent market for Libra-compatible wallets from which Calibra's rivals may be foreclosed. Other potential theories of harm (equally linked to well-known categories) would be the use of the network's governance rules to exclude operators that are not members to the developers' consortium, the charging of excessive or predatory commissions, or even the combination of Libra, Facebook and WhatsApp users' data without their express consent à la Bundeskartellamt's Facebook case.

REFERENCES:

Catalini, C., Gans, J. S. (2016), Some simple economics of the blockchain, Working Paper 22952, National Bureau of Economic Research.

Crémer, J., De Montjoye, Y.-A., Schweitzer, H. (2019), Competition policy for the digital era, Publications Office of the European Union.

Evans, D. S. (2008), Competition and Regulatory Policy for Multi-sided Platforms with Applications to the Web Economy, 2 Concurrences, 57-62.

Lianos, I. (2018), Blockchain competition, Centre for Law, Economics and Society Research Paper Series 4/2018, University College London.

Massarotto, G. (2020), Antitrust in the blockchain era, Notre Dame Journal of Emerging Technologies, 252-278.

Organisation for Economic Co-operation and Development (2018), Blockchain Technology and Competition Policy, Issues paper by the Secretariat, Directorate for Financial and Enterprise Affairs Competition Committee, April.

Schrepel, T. (2020), Libra: A Concentrate of "Blockchain Antitrust", 118 Michigan Law Review, 160-169.

Schrepel, T. (2020), The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems, 50 Pages, Harvard University (Berkman Center), Utrecht University School of Law, University Paris 1 Panthéon-Sorbonne, January.

Schrepel, T., Buterin, V. (2020), Blockchain code as antitrust.

Solano, P. (2017), EU Competition Law needs to install a plug-in, 40(3) World Competition, 393–420.

La irreversibilidad del hash y sus implicaciones en materia **de privacidad**

Sara Esclapés. Iñigo García de la Mata. Oscar Delgado
Abogados. Grant Thornton

Las bases de datos descentralizadas, la criptografía o los protocolos peer to peer son tecnologías y técnicas tradicionales que, combinadas de forma específica, han dado lugar a lo que se conoce actualmente como tecnología Blockchain. De entre las técnicas utilizadas en el marco de la cadena de bloques destaca la utilización de la función hash, que se ha convertido en uno de los pilares fundamentales que garantizan la integridad de la información y que permite, en combinación con el resto del sistema, el salto definitivo hacia el Internet del Valor.

La compatibilidad de función hash con las normas relativas a protección de datos ha sido analizada exhaustivamente a lo largo de los últimos años a raíz de la popularización de aplicaciones basadas en Blockchain. En concreto, el análisis se ha centrado en el estudio del cumplimiento del principio de confidencialidad y seguridad, así como en el riesgo de reidentificación de personas físicas a partir de los hashes registrados en Blockchain.

El hash es el resultado de aplicar un algoritmo a un dato o conjunto de datos. Este algoritmo es conocido con el nombre de función hash. La función hash devuelve un resultado de tamaño fijo predeterminado (un código alfanumérico, en esencia, un código de bits) a partir de un valor de entrada o conjunto de valores de entrada de cualquier tamaño.

La función hash se diseña cumpliendo con las siguientes especificaciones:

- **Dependencia de bit:** una función hash está diseñada para asegurar que cada bit de salida de la función dependa de cada bit de entrada.
- **Efecto avalancha:** un cambio en un solo bit en la entrada (de 0 a 1 o viceversa) produce un gran cambio en el estado interno del algoritmo y en el valor de hash final (valores de salida). Dado que la salida cambia tan drásticamente con cada variación de un bit de entrada, se impide la construcción de relaciones entre entradas y salidas (o partes de ellas).

- **No linealidad:** las funciones hash siempre contienen operaciones no lineales, evitándose las aplicaciones algebraicas para resolver hashes inversos o recalcular la salida del hash.

La conclusión que se deriva de estas especificaciones es que el resultado de aplicar la función hash a un dato o conjunto de datos no es independiente de estos, sino que dicho resultado se deriva o depende del conjunto de datos utilizados como entrada. En otras palabras, la función hash utiliza la propia información de entrada como valor de entropía, junto con operaciones no lineales. De esta forma se perturba la información consigo misma y la posibilidad de generar mecanismos que calculen el hash de forma más eficiente que la propia función se vuelven complejos.

En el marco de la tecnología Blockchain, la función hash se utiliza para garantizar la integridad de la información. En muchas ocasiones, y especialmente en contextos donde opera una identidad digital de personas físicas, el hash puede referirse a una credencial, una transacción o un atributo concreto de un individuo. Es en estos casos donde opera el concepto de seudonimización.

Desde el punto de vista jurídico y con arreglo a la Opinión 5/2014 del ya extinto Grupo de Trabajo del Artículo 29, la función hash es una técnica de seudonimización. La razón por la cual se le otorga tal condición es que, a pesar de que se trata de una función no reversible, si se conoce el rango de los valores de entrada de la función, estos pueden introducirse uno a uno a fin de obtener el valor real de un registro determinado. Lo anterior implica que los hashes representativos de la información personal podrían eventualmente ser considerados datos personales si existe alguna forma de relacionarlos con una persona física en concreto y, por tanto, encontrarse sometidos a la normativa de protección de datos personales, tal y como se deriva del artículo 4.5 del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante "RGPD") y del considerando 26 del mismo texto.

Para determinar si los datos seudónimos son susceptibles de considerarse datos personales, el RGPD utiliza un enfoque basado en el riesgo de identificación. Allá donde, considerando medios y factores objetivos, exista riesgo de identificación del titular de un dato o conjunto de datos seudónimos, estos deberán considerarse datos personales y por tanto sujetos al RGPD. Por el contrario, si el riesgo de identificación, teniendo en cuenta medios y factores objetivos, es reducido, los datos podrán tratarse como datos anónimos, aunque la probabilidad de identificación no pueda ser excluida con absoluta certeza.

Aunque para estudiar el riesgo de reidentificar a una persona física a través de hashes debe atenderse a múltiples variables como la vinculación del hash a otros identificadores, la repetición del mismo hash a lo largo de la cadena, el espacio de mensajes, etc. (ver informe de la AEPD "Introducción al hash como técnica de seudonimización"), nuestro estudio se centra en el análisis concreto de la propia función hash.

¿Hasta qué punto tomando únicamente el resultado de la función hash puede este considerarse un dato con un grado suficiente de anonimización si se desconocen los valores de entrada originales de la función? ¿Cómo garantizar que esta técnica cumple con el principio de confidencialidad y seguridad?

La robustez de una función hash puede medirse a partir de las siguientes premisas:

- **Resistencia a primera preimagen:** es la posibilidad de, partiendo de un hash, hallar el conjunto de datos original que generó ese hash. Esto suele producirse a través del uso de diccionarios y/o fuerza bruta. Un ataque por fuerza bruta consiste en probar todas las combinaciones de datos de entrada posibles hasta encontrar el hash asociado. En otras palabras, si se conoce información acerca de las características de los valores de entrada de la función hash, se pueden realizar intentos sucesivos, probando conjuntos de datos en la función hasta obtener el valor real de un registro determinado. Por tanto, cuanto mayor sea el grado de información disponible acerca de los datos que el hash representa y, por tanto, más limitado se encuentre el universo de posibles datos de entrada,

más sencillo resultará encontrar los valores que dieron lugar al hash.

Una función hash no resistente a la primera preimagen permitiría encontrar un conjunto de resultados equiprobables como valores de entrada. En consecuencia, y en función del grado de conocimiento del contexto de la información registrada en la red, será posible inferir el dato correcto del conjunto de resultados equiprobables e incluso singularizar al individuo ya sea de forma directa o indirecta.

- **Resistencia a la segunda preimagen:** es la posibilidad de, dado un conjunto de datos inicial y su hash, hallar un nuevo conjunto de datos que tenga exactamente el mismo hash que el conjunto original. Aunque esta cuestión, en principio, no afectaría a la privacidad, ya que se parte del supuesto de que los datos iniciales se conocen, sí resulta esencial en términos de seguridad. Una función hash con baja resistencia a la segunda preimagen, sería altamente vulnerable y permitiría encontrar otra combinación de elementos que resultasen en el mismo hash. La garantía de integridad del hash quedaría vulnerada pues datos de entrada distintos darían lugar a un hash idéntico.

- **Resistencia a colisiones:** es la posibilidad de hallar un conjunto de datos que tengan el mismo hash. Nótese que la diferencia entre segunda preimagen y colisión es que, en el caso anterior, se cuenta tanto con el conjunto de datos inicial como con el hash. En el caso de las colisiones solamente se cuenta con el hash, por lo que el universo de combinaciones posibles es mucho mayor. Si un conjunto de datos es resistente a colisiones, entonces es resistente a segunda preimagen. Una función hash no resistente a colisiones generaría problemas tanto de privacidad, por permitir encontrar conjuntos de datos de entrada a partir de los cuales inferir el resultado, como de seguridad, tal y como se indicó en el punto anterior.

Los algoritmos avanzan y evolucionan a un ritmo vertiginoso. Por tanto, ¿cómo medir si una función hash es resistente a los tres problemas anteriores? La respuesta a esta pregunta parte de un esquema de horizonte temporal. Cuando el tiempo computación requerido para resolver estos tres problemas es tan alto que el hash resulta "computacionalmente intratable" podríamos afirmar que la función es resistente. El término "computacionalmente intratable", en esencia, significa que el tiempo que lleva resolver estos problemas a un procesador es tan alto que, en la práctica, resultan imposibles de resolver o que, de resolverse, la información ya no resultaría útil en ese momento. El significado de "computacionalmente intratable" puede variar en función del tiempo de vida del dato y de los medios disponibles en cada momento. En consecuencia, y con arreglo a lo dispuesto en el considerando 26 RGPD la resistencia de la función debe analizarse en cada caso concreto tomando en consideración el tipo de dato y factores objetivos como costes y tiempo necesarios para la identificación, así como la tecnología disponible tanto actualmente como en el futuro. Para analizar esta última cuestión, resulta útil tomar como referencia la Ley de Moore.

La Ley de Moore es la norma que, durante cinco décadas, ha marcado el destino de los procesadores y chips que soportan los equipos tecnológicos. Se trata de una ley empírica, formulada por el cofundador de Intel, Gordon E. Moore, el 19 de abril de 1965, cuyo cumplimiento se ha podido constatar hasta hoy.

Esta regla establece que, cada dos años, se duplica el número de transistores que caben en un circuito integrado o, en otras palabras, con el paso del tiempo, la tecnología tiende a multiplicar su rendimiento y a dividir su coste.

Hasta hoy la teoría se ha cumplido (con pocas excepciones) pero inevitablemente la posibilidad de aumentar la capacidad y reducir el tamaño de los chips tiene un límite. Por este motivo, se prevé que la curva de la Ley de Moore se estanque en la próxima década. Ello podría tener consecuencias positivas en términos de privacidad ya que, si un hash es computacionalmente intratable con los medios disponibles actualmente, es muy posible que siga siendo computacionalmente intratable en el futuro a medio plazo. Esto permitiría analizar el riesgo asociado a la reidentificación a través de la tecnología disponible con mayor rigor.

No obstante, no cabe perder de vista la posibilidad de que la computación cuántica irrumpa en el ecosistema en un futuro a medio plazo. En este caso, la curva de la Ley de Moore tomaría una forma diferente y, por tanto, las posibilidades de considerar un hash como computacionalmente intratable quedarían drásticamente reducidas.

Por lo tanto, y en línea con lo ya señalado por la AEPD, las soluciones más recomendables para enfrentar los tres problemas mencionados anteriormente parten de la base de la aplicación de medidas que refuercen la dificultad de atacar la función hash. Algunos de los ejemplos más conocidos son cifrar los datos antes o después de aplicarles la función o utilizar técnicas de "salt" y "pepper". Dichas medidas, deben ser combinadas con revisiones periódicas de la función, ponderando, caso por caso, el tiempo de vida del dato, su sensibilidad y la tecnología disponible en el momento actual y futuro.

El objetivo no es otro que reducir la probabilidad razonable de reidentificar a personas físicas, incrementando el nivel de esfuerzo necesario para una recreación exitosa del contenido original del hash, garantizando en mayor medida el cumplimiento de los principios recogidos en el RGPD.

REFERENCIAS:

AEPD (2019), La K anonimidad como medida de la privacidad. https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

AEPD (2019), Introducción al hash como técnica de seudonimización https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

Article 29 Working Party (2014), Opinion 5/2014 on Anonymisation Techniques https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

CNIL (2018), Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Ed Felten (2012), Does hashing make data Anonymous? Federal Trade Commission https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous

EPRS (2019), Blockchain and the General Data Protection Regulation, can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

European Union blockchain observatory and forum (2018), Blockchain and the GDPR.https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Finck, M. and Pallas, F. (2020), They who must not be identified- distinguishing personal from non-personal data under GDPR. International Data Privacy Law, Vol. 0, No. 0 https://academic.oup.com/idpl/article/10/1/11/5802594

Holmgren, J. and Lombardi, A. (2018), Cryptographic Hashing from Strong One-Way Functions. IEEE 59th Annual Symposium on Foundations of Computer Science.

Lucks, S. (2004), Design Principles for Iterated Hash Functions. https://pdfs.semanticscholar.org/ac6f/5fa8d954d64c3fc8f01f866c6824ef3d502c.pdf

Talbot, D. Welsh, J. (2010), One-way functions. Complexity and Cryptography, pp. 125–140.

The irreversibility of hash and its implications **for privacy**

Sara Esclapés. Iñigo García de la Mata. Oscar Delgado
Lawyers. Grant Thornton

Decentralized databases, cryptography, or peer-to-peer protocols are traditional technologies and techniques that, combined, have resulted in the well-known Blockchain technology. Amongst the techniques used in Blockchain framework, hash function is one of the main cornerstones. It guarantees the integrity of the information and allows, in conjunction with the rest of the system, the final step towards the Internet of Value.

Compatibility between hash function and data protection regulation has been extensively studied over the past few years, in part, due to the popularization of Blockchain-based applications. Specifically, the analysis has focused on the compliance with the principle of confidentiality and security, as well as on the risk of reidentification of individuals from the hashes registered in Blockchain.

A hash is the result of applying an algorithm to a data or data set. This algorithm is known as a hash function. The hash function returns a result of a predetermined fixed size (an alphanumeric code, essentially a bit code) from an input value or set of input values of any size.

The hash function is designed to meet the following specifications:

- **Bit Dependency:** A hash function is designed to ensure that each output bit of the function is dependent on each input bit.

- **Avalanche effect:** refers to the fact that a change in a single bit at the input (from 0 to 1 or vice versa) results in a large change in the internal state of the algorithm and in the final hash value (output values). Since the output changes so drastically with every variation of an input bit, the construction of relations-

hips between inputs and outputs (or parts of them) is prevented.

- **Non-linearity:** hash functions always contain non-linear operations, avoiding algebraic applications to solve inverse hashes or recalculate the hash output.

The conclusion derived from the specifications above is that the result of applying the hash function to a data or data set is dependent on the data set used as input. In other words, the hash function uses the input information itself as an entropy value, along with non-linear operations. Thus, the information is disturbed with itself and the possibility of generating mechanisms that calculate the hash more efficiently than the function becomes complex.

Within the framework of the Blockchain technology, hash function is used to ensure the integrity of the information. In many cases, and especially in contexts where a digital identity belonging to a natural person operates, the hash may refer to a credential, a transaction, or an attribute of an individual. In these cases, the concept of pseudonymization becomes relevant.

From a legal point of view and according to Opinion 5/2014 of the now extinct Article 29 Working Party, the hash function is a pseudonymization technique. The reason lies on the fact that, although it is a non-reversible function, if the range of input values of the function is known, they can be entered one by one in order to obtain the actual value of a given record. This implies that hashes representing personal information could eventually be considered as personal data if there is some way to relate them to a specific natural person. Therefore hashes could be subject to data protection rules, as derived from Article 4(5) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR") and from recital 26 of the same text.

To determine whether pseudonymous data can be considered personal data, the GDPR uses a risk-based approach. When, considering objective means and factors, there is a risk of identification of the holder of a data or set of pseudonymous data, these should be considered personal data and therefore subject to the GDPR. On the contrary, if the risk of identification, considering objective means and factors, is low, the data may be treated as anonymous data, although the probability of identification cannot be excluded with absolute certainty.

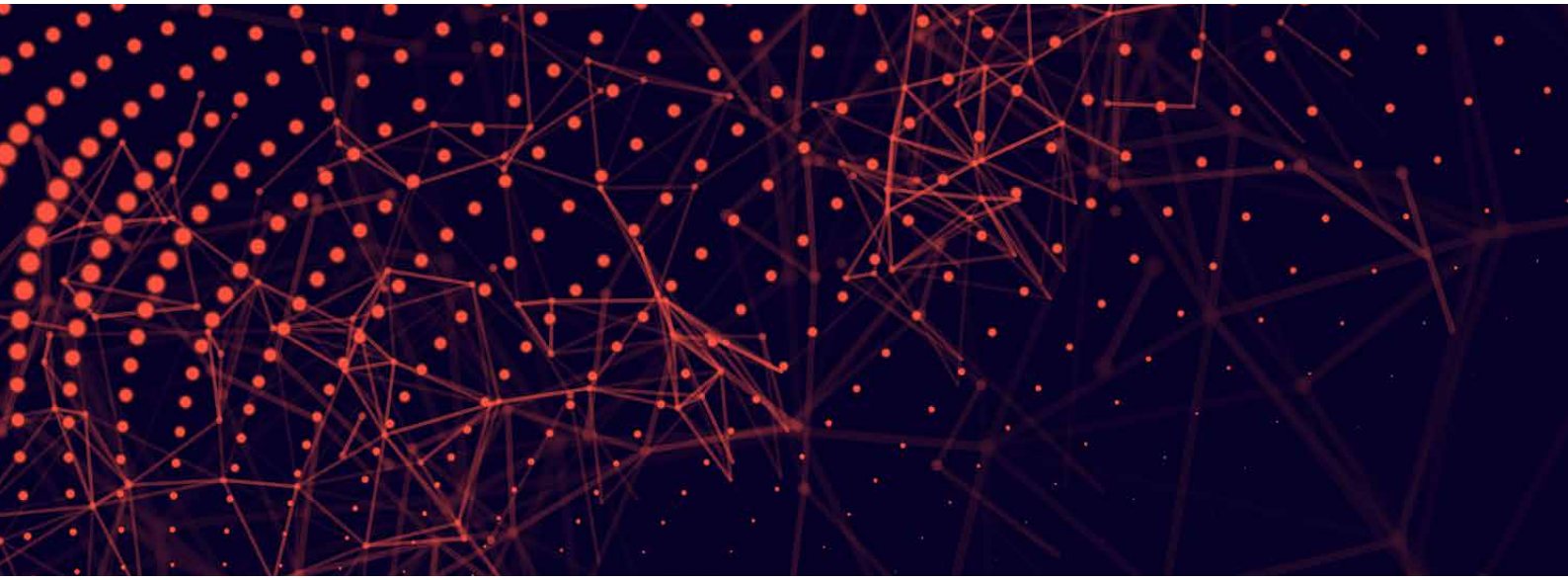
Even though when studying the risk of reidentifying a natural person through hashes we must take into account multiple variables such as the linkage of the hash to other identifiers, the repetition of the same hash along the chain, the message space, etc. (see AEPD report "Introduction to hash as a pseudonymization technique"), our study focuses on the concrete analysis of the hash function itself.

To what extent can the result of the hash function alone be considered as data with a sufficient degree of anonymity if the original input values of the function are not known? How to ensure that this technique complies with the principle of confidentiality and security?

The robustness of a hash function can be measured on the basis of the following premises:

- **Resistance to first preimage:** it is the possibility of, starting from a hash, finding the original data set that generated that hash. This usually occurs using dictionaries and/or brute force attacks. A brute-force attack consists of trying all possible combinations of input data until the associated hash is found. In other words, if information about the characteristics of the input values of the hash function is known, successive attempts can be made, testing sets of data in the function until the actual value of a given record is obtained. Therefore, the greater the degree of information available about the data that the hash represents, and therefore the more limited the universe of possible input data is, the easier it will be to find the values that gave rise to the hash.

  A hash function not resistant to the first preimage would allow to find a set of compa-



rable results as input values. Consequently, and depending on the degree of knowledge of the context of the information recorded in the network, it will be possible to infer the correct data from the set of comparable results and even to single out the individual directly or indirectly.

- **Resistance to the second preimage:** it is the possibility of, given an initial data set and its hash, finding a new data set that has the same hash as the original set. Although this issue, in principle, would not affect privacy, since it is assumed that the initial data is known, it is essential in terms of security. A hash function with low resistance to the second preimage would be highly vulnerable and would allow to find combination of elements that would result in the same hash. The integrity guarantee of the hash would be breached as different input data would result in an identical hash.

- **Collision resistance:** it is the possibility of finding a data set that has the same hash. Note that the difference between second preimage and collision is that, in the previous case, both the initial data set and the hash are available. In the case of collisions, only the hash is available, so the universe of possible combinations is much larger. If a data set is collision resistant, then it is resistant to second preimage. A non-collision-resistant hash function would create both privacy problems, by allowing to find input datasets from which to infer the result, and safety problems, as discussed in the previous point.

Algorithms progress and evolve at a dizzying rate. So how to measure whether a hash function is resistant to the three problems above? The answer to this question is based on a time horizon scheme. When the computational time required to solve these three problems is so high that the hash is "computationally intractable" we could say that the function is resistant. The term "computationally intractable", in essence, means that the time it takes a processor to solve these problems is so high that, in practice, they are impossible to solve or that, if solved, the information would no longer be useful at that moment.

The meaning of "computationally intractable" may vary depending on the lifetime of the data and the means available at any given time. Consequently, and in accordance with the provisions of recital 26 of the GDPR, the strength of the function must be analyzed in a case by case basis taking into account the type of data and objective factors such as costs and time required for identification, as well as available technology now and in the future. To analyze the latter question, it is useful to take Moore's Law as a reference.

Moore's Law is the rule that, for five decades, has marked the fate of processors and chips that technological equipment support. It is an empirical law, formulated by Intel co-founder Gordon E. Moore on April 19, 1965, that has been observed until today.

This rule states that, every two years, the number of transistors that fit into an integrated circuit doubles, or in other words, over time, the technology tends to multiply its performance and divide its cost.

Until today, the theory has been fulfilled (with few exceptions) but inevitably the possibility of increasing capacity and reducing chip size has a limit. For this reason, Moore's Law curve is expected to stagnate in the next decade. This could have positive consequences in terms of privacy because, if a hash is computationally intractable with the means available today, it is quite possible that it will remain computationally intractable in the medium-term future. This would allow the risk associated with reidentification through available technology to be analyzed more rigorously.

However, we should not lose sight of the possibility that quantum computing will break into the ecosystem in the medium-term future. In this case, the Moore's Law curve would take a different shape and, therefore, the possibilities of considering a hash as computationally intractable would be drastically reduced.

Therefore, and in line with what has already been pointed out by the AEPD, current solutions to face the three problems stated above must be based on measures that reinforce security of the hash function. Most known examples could be encrypting the data before or after hashing it or adding salt or pepper techniques. This, of course, should be combined with periodical tests of the function, pondering, in each case, the life of the data, its sensitivity and available technological advances both existing and expected in the future.

The objective is none other than to reduce the reasonable probability of re-identifying individuals, increasing the level of effort required for a successful recreation of the original hash content, further guaranteeing compliance with the principles set out in the GDPR.

REFERENCES:

AEPD (2019), La K anonimidad como medida de la privacidad. https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

AEPD (2019), Introducción al hash como técnica de seudonimización https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

Article 29 Working Party (2014), Opinion 5/2014 on Anonymisation Techniques https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

CNIL (2018), Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Ed Felten (2012), Does hashing make data Anonymous? Federal Trade Commission https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous

EPRS (2019), Blockchain and the General Data Protection Regulation, can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

European Union blockchain observatory and forum (2018), Blockchain and the GDPR.https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Finck, M. and Pallas, F. (2020), They who must not be identified- distinguishing personal from non-personal data under GDPR. International Data Privacy Law, Vol. 0, No. 0 https://academic.oup.com/idpl/article/10/1/11/5802594

Holmgren, J. and Lombardi, A. (2018), Cryptographic Hashing from Strong One-Way Functions. IEEE 59th Annual Symposium on Foundations of Computer Science.

Lucks, S. (2004), Design Principles for Iterated Hash Functions. https://pdfs.semanticscholar.org/ac6f/5fa8d954d64c3fc8f01f866c6824ef3d502c.pdf

Talbot, D. Welsh, J. (2010), One-way functions. Complexity and Cryptography, pp. 125–140.

El desarrollo de las **técnicas de anonimización** y su aplicación en el blockchain

Sonia Vázquez. Abogada. Castroalonso

En lo que al tratamiento de datos de carácter personal en el uso de tecnologías blockchain se refiere, la CNIL recuerda y se remite al principio de minimización establecido en el RGPD, el cual exige que la información de carácter personal que vaya a ser tratada quede limitada a aquella que resulte pertinente y necesaria para llevar a cabo las finalidades de tratamiento concretas para las cuales fue recabada. Es decir, con el fin de que se cumpla con lo dispuesto en el RGPD, el tratamiento de datos personales en una transacción blockchain debería limitarse a aquellos estrictamente necesarios para la realización de la misma, previa aplicación del principio de privacidad desde el diseño y por defecto (art. 25 RGPD). De esta forma, se analizará el tratamiento detalladamente, de tal modo que se verifique si el tratamiento de información personal a través de la tecnología blockchain es pertinente y, ajustado a Derecho.

En el caso de que se confirme la necesidad de tratar datos de carácter personal en una operación blockchain, y con el fin de garantizar la seguridad en el tratamiento, se deberá tener en cuenta lo dispuesto en el artículo 32 RGPD, el cual exige a los responsables y encargados del tratamiento que apliquen las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que, entre otras medidas, incluyendo la seudonimización y el ci-

frado de datos personales de tal modo que se pueda garantizar la confidencialidad, la integridad, disponibilidad y resiliencia permanente de los sistemas y servicios, confirmando la capacidad de restaurar la disponibilidad de los datos y la seguridad en el tratamiento.

Encontrándonos en un punto en el que resulta de vital trascendencia no solamente proteger las comunicaciones, sino también el contenido de estas, especialmente en lo que a datos personales se refiere, se plantea muy atractivo el uso de técnicas de anonimización, recordando que, en estos casos, el RGPD no aplicaría sobre los datos anónimos tal y como se detalla en el Considerando 26 RGPD. En los últimos años, las técnicas de anonimización han ido cobrando cada vez más importancia en el ámbito de la sociedad de la información, al conjugar la posibilidad de que los novedosos desarrollos tecnológicos puedan seguir avanzando sin que, por ello, se menoscabe la protección de los datos personales. Sin embargo, es importante subrayar que las técnicas de anonimización utilizadas deberán ser lo suficientemente robustas para garantizar la imposibilidad de reidentificar al titular de los datos, así como la irreversibilidad del proceso. Los datos ofuscados a través de técnicas de seudonimización, como el cifrado reversible que permite codificar un contenido transformándolo en información ininteligible que únicamente podrá ser descifrado por aquel que disponga de las claves de cifrado correspondientes, distinguiendo entre claves iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida), o bien las funciones hash criptográficas (funciones que cumplen una serie de propiedades que las hacen idóneas para dotarse de seguridad y, por tanto, ser utilizadas en el área de la criptografía) que puedan ser revertidas, seguirán teniendo la consideración de datos personales.

Concretando, un algoritmo de hash por sí solo no es suficiente para hacer irreversible la anonimización, ya que pequeñas cadenas de texto como los microdatos, pueden ser fácilmente reidentificables con un programa informático que genere cifras consecutivas y sus correspondientes huellas digitales. A lo largo de las últimas décadas, se han llevado a cabo importantes avances sobre las técnicas de anonimización, entre las que destaca la utilización de algoritmos criptográficos orientados a verificar la veracidad de una información sin que exista la necesidad de compartir los datos que la componen, logrando de esta forma un proceso de anonimización muy robusto. Estaríamos ante la encriptación homomórfica funcional (cuyo origen se encuentra en los años 70) o las Zero-knowledge proofs (ZKP).

La encriptación homomórfica es una técnica que permite realizar operaciones sobre los datos cifrados y obtener resultados, también cifrados, equivalentes a las operaciones realizadas directamente sobre la información original. Esta técnica permite que la información codificada pueda compartirse con terceros y que sea utilizada en procesos computacionales sin que los sistemas implicados accedan de forma efectiva a la información de carácter personal pero sí operar en base a los cálculos y procesos facilitados. Pueden distinguirse tres tipos de cifrado homomórfico: Parcial cuando el tipo de operaciones es limitado, o PHE (Partial Homomorphic Encryption), medio o SHE (Somewhat Homomorphic Encryption) y completo o FHE (Full Homomorphic Encryption).

La evolución del esquema de cifrado homomórfico completo a lo largo de estas décadas, abre la posibilidad del tratamiento de datos personales anonimizados garantizando la privacidad y que los resultados de los tratamientos sean accesibles únicamente al poseedor de la clave de descifrado.

Por su parte, la Zero Knowledge Proof (ZKP) podría definirse como "un protocolo que permite que un "probador" convenza a un "verificador" de que el primero tiene información secreta verificable. Todo ello sin permitir que el verificador sepa algo sobre dicha información. La información secreta, puede ser verificable estadísticamente o de manera determinística. Y sólo uno de ellos, el verificador o el probador, necesitan contar con recursos limitados[1]".

Es decir, estaríamos ante un método criptográfico que permitiría mantener un secreto criptográficamente protegido y al mismo tiempo, permitiría demostrar a terceros que dicho secreto existe, pudiendo estos validarlo en cualquier momento.

Sin perjuicio de que aún existan limitaciones en la aplicación práctica de estas tecnologías, se plantean como medios criptográficos con gran potencial para alcanzar altos niveles de seguridad, privacidad y anonimato de los usuarios, garantizando transacciones seguras. En este sentido, los criptógrafos han hecho grandes avances en la aplicación de esta tecnología. Nos encontramos ante un escenario muy prometedor que ofrecerá múltiples posibilidades en el tratamiento de datos personales e información sensible a través de transacciones blockchain, no solo en el ámbito privado, sino también la Administración Pública, permitiendo la externalización totalmente segura de computaciones privadas, sistemas basados en la nube y redes descentralizadas y distribuidas.

Habrá, por tanto, que seguir muy de cerca todos los avances y desarrollos tecnológicos en esta materia, hasta que los algoritmos se conviertan en estándares que posibiliten su implementación de una forma fluida y general.

REFERENCIAS:

AEPD (2020). Cifrado y Privacidad III: Cifrado Homomórfico. https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico

AEPD (2016). Introducción al hash como técnica de seudonimización de datos personales. https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

AEPD (2016). Orientaciones y garantías en los procedimientos de anonimización de datos personales. https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

Alameda T. (2020). Zero Knowledgement Proof. BBVA Tecnología. https://www.bbva.com/es/zero-knowledge-proof-como-preservar-la-privacidad-en-un-mundo-basado-en-datos/

Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Brassard G., Chaum D., Crépeau C. (1988). Minimum Disclosure Proofs of Knowledge. JOURNAL OF COMPUTER AND SYSTEM SCIENCES 37, Pages: 156-189. http://crypto.cs.mcgill.ca/~crepeau/PDF/BCC88-jcss.pdf

CNIL (2018). Blockchain. Premiers éléments d'analyse de la CNIL. https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

Herrera Herrera, F. (2019). Blockchain, anonimización y Reglamento General de Protección de Datos. Blog Editorial Jurídica Sepin. https://blog.sepin.es/2019/04/blockchain-anonimizacion-rgpd/Informe

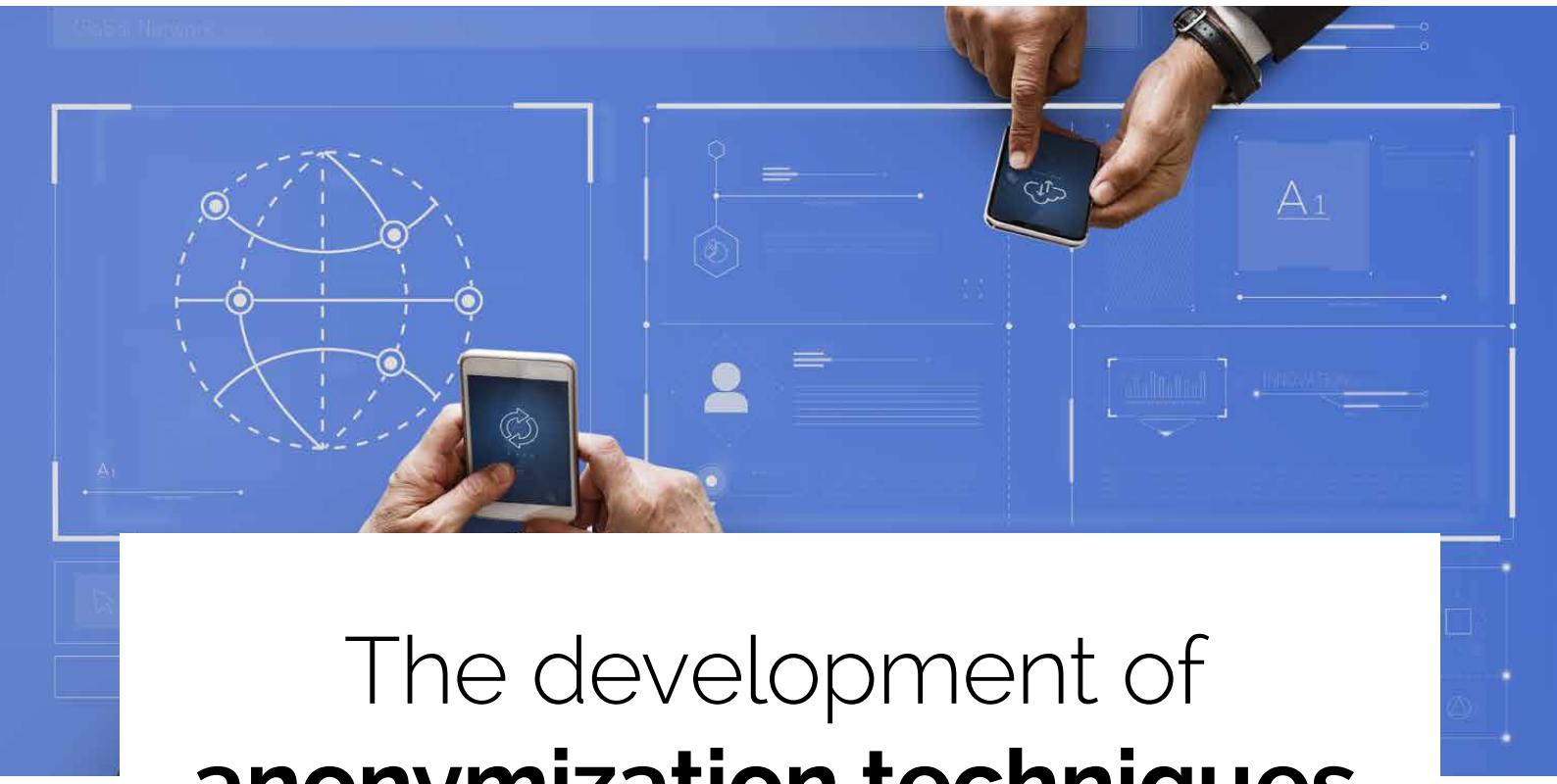
INCIBE (2016). Estudio en el mercado de la Ciberseguridad. https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

Kundro, D. (2019). Criptografía homomórfica: un paradigma de cifrado cada vez más cercano. Welivesecurity. https://www.welivesecurity.com/la-es/2019/09/04/criptografia-homomorfica-paradigma-cifrado-cercano/

Lauter K., Naehrig M. and Vaikuntanathan V. (2011). Can Homomorphic Encryption be Practical?. Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. Pages: 113-124. https://eprint.iacr.org/2011/405.pdf

The European Union Blockchain Observatory and Forum (2018). Blockchain and the GDPR. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[1] *Minimum Disclosure Proofs of Knowledge – Gilles Brassard; David Chaum; Claude Crépeau, 1987.*



The development of **anonymization techniques** and their application in the use of blockchain

Sonia Vázquez. Lawyer. Castroalonso

Regarding the processing of personal data in the use of blockchain technologies, the CNIL refers to the principle of minimization established in the RGPD; it requires that the personal information that is going to be processed is limited to that which is relevant and necessary to carry out the specific processing purposes for which it was collected.

In order to comply with the provisions of the RGPD, the processing of personal data in a transaction in a blockchain network should be limited to those strictly necessary to carry it out, after applying the principle of privacy by design and by default (art. 25 RGPD).

In this way, the processing will be analysed in detail, in such a way that it is verified if the processing of personal information through blockchain technology is pertinent and adjusted to the Law.

Confirmed the need to process personal data in a blockchain operation, the provisions settled in article 32 RGPD must be taken into account in order to guarantee the security of processing. It requires that data controllers and data processors to apply the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk that, among other measures, including the pseudonymisation and encryption of personal data in such a way that

confidentiality, integrity, permanent availability and resilience of systems and services, confirming the ability to restore data availability and processing security.

Finding ourselves at a point in which it is vitally important not only to protect communications, but also their content, especially regarding personal data, the use of anonymization techniques may be seen as a very attractive possibility, remembering that, in these cases, GDPR would not apply to anonymous data as detailed in Recital 26 of RGPD.

In recent years, anonymization techniques have become increasingly important in the field of the information society, combining the possibility that novel technological developments can go any further without therefore, undermining the protection of personal data.

However, it is important to underline that the anonymization techniques used must be robust enough to guarantee the impossibility of re-identifying the owner of the data, as well as the irreversibility of the process.

Data masked through pseudonymisation techniques, such as reversible encryption that allows content to be encoded, transforming it into unintelligible information that can only be decrypted by someone who has the corresponding encryption keys, distinguishing between the same keys (symmetric cryptography), different (asymmetric cryptography) or of both types (hybrid cryptography), or cryptographic hash functions (functions that fulfill a series of properties that make them ideal for providing security and, therefore, be used in the area of cryptography) that can be reversed, they will continue to be considered personal data.

In other words, a hash algorithm is not enough to make anonymization irreversible, since small text strings such as microdata can be easily re-identifiable with a computer program that generates consecutively running numbers and their corresponding fingerprints.

Over the last several decades, important advances have been made on anonymization techniques, among which the use of cryptographic algorithms aimed at verifying the veracity of information without the need to share the data that compose it stands out, thus achieving a very robust anonymization process. We would be facing functional homomorphic encryption (whose origin is in the 70s) or the Zero-knowledge proofs (ZKP).

Homomorphic encryption is a technique that allows operations to be carried out on encrypted data and to obtain results, also encrypted, equivalent to operations carried out directly on the original information. This technique allows coded information to be shared with third parties and be used in computational processes without the systems involved effectively accessing the personal information but operating on the basis of the calculations and processes provided. Three types of homomorphic encryption can be distinguished: Partial when the type of operations is limited, or PHE (Partial Homomorphic Encryption), medium or SHE (Somewhat Homomorphic Encryption) and full or FHE (Full Homomorphic Encryption).

The evolution of the complete homomorphic encryption scheme throughout these decades opens the possibility of anonymized personal data processing, guaranteeing privacy and that the results of the processing may be limited only to the holder of the decryption key.

For its part, Zero Knowledge Proof (ZKP) could be defined as "protocols that are given for allowing a "prover" to convince a "verifier" that the prover knows some verifiable secret information, without allowing the verifier to learn anything about the secret. The secret can be probabilistically or deterministically verifiable, and only one of the prover or the verifier need have constrained resources. This paper unifies and extends models and techniques previously put forward by the authors and compares some independent related work"[1].

We would be facing a cryptographic method that would allow to maintain a cryptographically protected secret and, at the same time, it would allow to demonstrate to third parties that the aforementioned secret exists, being able to validate it at any moment.

Notwithstanding the fact that there are still limitations in the practical application of these technologies, they are considered as cryptographic means with great potential to achieve high levels of security, privacy and anonymity for users, guaranteeing safe transactions. In this regard, cryptographers have made great strides in applying this technology. We are facing a very promising scenario that will offer multiple possibilities in the processing of personal data and sensitive information through blockchain transactions not only in the private sphere, but also in the Public Administration. It will allow the totally secure outsourcing of private computing, cloud-based computing models and decentralized and distributed networks.

Therefore, it will be necessary to closely monitor all technological advances and developments in this matter, until the algorithms may become standards that enable their implementation in a smooth and general way.

REFERENCES:

AEPD (2020). Cifrado y Privacidad III: Cifrado Homomórfico. https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico

AEPD (2016). Introducción al hash como técnica de seudonimización de datos personales. https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

AEPD (2016). Orientaciones y garantías en los procedimientos de anonimización de datos personales. https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

Alameda T. (2020). Zero Knowledgement Proof. BBVA Tecnología. https://www.bbva.com/es/zero-knowledge-proof-como-preservar-la-privacidad-en-un-mundo-basado-en-datos/

Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Brassard G., Chaum D., Crépeau C. (1988). Minimum Disclosure Proofs of Knowledge. JOURNAL OF COMPUTER AND SYSTEM SCIENCES 37, Pages: 156-189. http://crypto.cs.mcgill.ca/~crepeau/PDF/BCC88-jcss.pdf

CNIL (2018). Blockchain. Premiers éléments d'analyse de la CNIL. https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

Herrera Herrera, F. (2019). Blockchain, anonimización y Reglamento General de Protección de Datos. Blog Editorial Jurídica Sepin. https://blog.sepin.es/2019/04/blockchain-anonimizacion-rgpd/Informe

INCIBE (2016). Estudio en el mercado de la Ciberseguridad. https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

Kundro, D. (2019). Criptografía homomórfica: un paradigma de cifrado cada vez más cercano. Welivesecurity. https://www.welivesecurity.com/la-es/2019/09/04/criptografia-homomorfica-paradigma-cifrado-cercano/

Lauter K., Naehrig M. and Vaikuntanathan V. (2011). Can Homomorphic Encryption be Practical?. Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. Pages: 113-124. https://eprint.iacr.org/2011/405.pdf

The European Union Blockchain Observatory and Forum (2018). Blockchain and the GDPR. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[1] *Minimum Disclosure Proofs of Knowledge – Gilles Brassard; David Chaum; Claude Crépeau, 1987.*

Euro Digital: contexto y perspectivas regulatorias

Pablo Sanz Bayón
Profesor de Derecho Mercantil, ICADE

1. INTRODUCCIÓN: EL PORQUÉ DE LAS MONEDAS DIGITALES DE BANCA CENTRAL (CBDC)

El ecosistema de la economía digital ha dado lugar en los últimos años a la proliferación de una multiplicidad de nuevos medios de pago, intermediarios y plataformas. Entre los actores que comienzan a tener un papel destacado se encuentra el sector de las monedas virtuales, y en concreto, dentro del mismo, el de las criptomonedas, sobresaliendo entre ellas el Bitcoin. Como es sabido, estos activos digitales o tokens se caracterizan por usar una infraestructura cibernética y criptográfica de registro distribuido (DLT/Blockchain), que supone la descentralización y anonimato de las relaciones económicas y de los pagos (P2P). Como consecuencia de la innovación financiera que esta tecnología digital y sus actores están generando, los sistemas monetarios y bancarios de todo el mundo han comenzado a reaccionar ante este desafío[1].

La digitalización de formas alternativas de dinero, es decir, la aparición de criptoactivos con función de pago, es en efecto un reto frontal a la política monetaria tradicional. Además, el auge de esta innovación informática ha sido coetáneo y se ha retroalimentado por razón de la crisis económica mundial, sin precedentes en la historia moderna. Una crisis originada en 2008 que ha tratado de ser neutralizada mediante una política de expansión de la oferta monetaria, potenciada extraordinariamente en el primer semestre de 2020, como medida para estimular la demanda. Esta situación ha conducido al sistema financiero a unos tipos de

interés situados en niveles muy bajos, nulos o incluso negativos, lo que a su vez ha ido despertando el atractivo de los inversores por activos más rentables, como las criptomonedas.

El devenir de estos acontecimientos ha propiciado en los últimos meses el desarrollo de investigaciones sobre monedas virtuales de banca central, las denominadas Central Bank Digital Currencies (CBDC), en el que la conservación de la soberanía monetaria del Estado se sitúa en el centro del debate[2]. Lo que se plantea como un escenario hipotético podría dar lugar a un verdadero riesgo sistémico si la tendencia no se corrige por las autoridades y una mayoría de la población mundial va migrando y cambiando sus depósitos en dinero fíat hacia formas digitales alternativas, como son las criptomonedas descentralizadas o las monedas virtuales corporativas (stablecoins como Libra, del consorcio liderado por Facebook). La aparición de ecosistemas de comercio electrónico, con sus respectivos marketplaces globales y gigantescas comunidades de usuarios, con aplicaciones móviles operadas por multitud de proveedores de servicios de pago, de cambio y de custodia de monederos electrónicos desplazaría del mercado a la banca comercial y situaría el tráfico monetario fuera del perímetro de control de las autoridades supervisoras. En este contexto, la arquitectura financiera internacional y sus postulados de estabilidad podrían quedar comprometidos si no se plantea una respuesta coordinada a nivel supranacional e intergubernamental sobre las criptomonedas, yendo más allá de los aspectos fiscales y de prevención del blanqueo de capitales. Por todo ello, una respuesta ante este desafío está comenzando a cristalizarse en proyectos institucionales sobre las CBDC[3]. El banco central sería su emisor y supondría un elemento esencial de la digitalización total del mercado de pagos, con intención de sustituir progresivamente al efectivo físico[4]. El cambio de paradigma podría

---

[1] Para un estudio preliminar sobre los retos de la digitalización del dinero, consúltese: Brunnermeier, M.K., Landeau, J.P. y James, H., "The Digitalization of Money", Universidad de Princeton, agosto de 2019 (https://scholar.princeton.edu/sites/default/files/markus/files/02c_digitalmoney.pdf).

[2] Fuera del entorno de la tecnología DLT/Blockchain hay alternativas, como el servicio FedNow, en EEUU, que se centra en mejorar la velocidad de los pagos. https://www.frbservices.org/financial-services/fednow/index.html

[3] El pasado mes de enero, el Foro Económico Mundial, junto con algunos de los principales bancos centrales del mundo, establecieron un conjunto de herramientas (toolkit) para la formulación de políticas sobre las CBDC. Véase a este respecto: WEF White Paper: "Central Bank Digital Currency Policy-Maker Toolkit", 22 de enero de 2020 (https://www.weforum.org/whitepapers/central-bank-digital-currency-policy-maker-toolkit). Como expresó la jefa de tecnología blockchain y registros distribuidos (DLT) del Foro Económico Mundial, Sheila Warren: "Dado el papel crítico que desempeñan los bancos centrales en la economía mundial, cualquier implementación de una CBDC, incluso potencialmente con tecnología blockchain, tendrá un profundo impacto a nivel nacional e internacional. Es imperativo que los bancos centrales procedan con cautela, con un análisis riguroso de las oportunidades y desafíos que se presentan".

[4] El director del BIS, Agustín Carstens, reconoció el pasado mes de marzo que la principal razón de la aceleración de estos proyectos se debe sin duda a la eclosión de las criptomonedas, y particularmente, a los proyectos de stablecoins, como Libra, impulsada por Facebook. Las stablecoins han sido examinadas pormenorizadamente por un grupo de trabajo del G7. Lo que está detrás de impulso a las CBDC es salvaguardar la soberanía monetaria ante la emergencia de estos activos digitales en la economía digital, acompañados de múltiples sistemas de pago e intercambio.

ser radical porque supondría separar la regulación del dinero de la regulación del sistema financiero.

El Banco de Pagos Internacionales (BIS), en una encuesta de este año, ha dicho que más del 80% de los 66 bancos centrales consultados han reconocido estar trabajando en proyectos de CBDC. Al responder sobre sus principales motivaciones, los bancos centrales muestran, sin embargo, algunas diferencias. Los bancos de países emergentes entienden las CBDC como un mecanismo orientado, sobre todo, a mejorar la eficiencia y seguridad de los pagos nacionales, y también para promover la inclusión financiera. Sin embargo, las economías avanzadas justifican sus investigaciones en CBDC principalmente en la seguridad de los pagos y la estabilidad financiera[5].

Los Estados que están tomando la delantera son aquellos emergentes que tienen más vulnerabilidades en materia de control de efectivo, con amplias capas sociales excluidas del sistema financiero, con dificultades en la prevención del blanqueo de capitales o que pueden permitirse, debido a su idiosincrasia, potenciar rápidamente la digitalización de sus servicios financieros. No obstante, el poder e influencia de los bancos centrales más grandes será el factor que a buen seguro marque determinantemente el desarrollo definitivo de las CBDC en los próximos tiempos. El Banco Central Europeo (BCE) se encuentra entre ellos, pero de momento no al nivel de su homólogo chino, el Banco Popular de China, que ya ha desarrollado y está probando un proyecto piloto sobre el Yuan Digital (DC/EP), que se vinculará 1:1 a la moneda nacional, el RenMinBi (RMB). Por contraste, en EEUU, el proyecto Digital Dollar, promovido por el expresidente de la CFTC, Christopher Giancarlo pero al margen de la Reserva Federal, se encuentra aún en una fase muy embrionaria, después de haberse desestimado su introducción legal a través de los programas de estímulos contra la crisis del coronavirus[6].

El mayor reto de los reguladores bancarios y monetarios es que la CBDC sea estable, es decir, que su oferta esté administrada y proporcione confianza para servir como medio de pago con capacidad de reemplazar progresivamente al efectivo físico. Es por ello por lo que el lanzamiento de una CBDC no sólo implica el surgimiento de un medio de pago tecnológicamente más avanzado sino también que la diversidad de enfoques regulatorios puede conllevar diferentes efectos sobre la política monetaria de un banco central y con respecto a su misión de garantizar la estabilidad financiera. Las CBDC vienen, en este sentido, a neutralizar el auge de las criptomonedas, cuya capitalización y difusión comienza a ser cada vez más considerable, aunque su utilidad por el momento no sea como medio de pago sino fundamentalmente como reserva de valor.

---

[5] Vid. BIS," Impending arrival – a sequel to the survey on central bank digital currency", BIS Papers, Nº 107, 2020 (https://www.bis.org/publ/bppdf/bispap107.pdf).

[6] El debate sobre una CBDC en EEUU fue alentado a propósito de un borrador de un proyecto de ley de estímulo ante los efectos económicos de la pandemia. Este proyecto de ley sugería el uso de un dólar digital para facilitar la distribución de los pagos de una manera rápida y sin contacto. Al final, la idea fue desestimada y desapareció del borrador final del proyecto de ley. Sobre el proyecto del Dólar Digital, véanse los artículos en The Wall Street Journal, "We Sent a Man to the Moon. We Can Send the Dollar to Cyberspace", 15 de octubre de 2019 y "Former Regulator Known as 'Crypto Dad' to Launch Digital-Dollar Think Tank", 16 de enero de 2020. Para hacer seguimiento de esta propuesta, véase: https://www.digitaldollarproject.org/

2. EL PROYECTO DEL BCE: EL EURO DIGITAL

Como ha reconocido el propio BCE, su motivación sobre el Euro Digital es la de estar preparado a nivel tecnológico y regulatorio para cuando se dé esta disrupción de modo completo[7]. De ahí que el BCE haya delegado en 5 bancos centrales europeos, en colaboración con el BIS, el estudio de la viabilidad de su CBDC mediante un proyecto de prueba de concepto "EuroChain" en la plataforma Corda, de R3 y con el apoyo de Accenture[8]. Este proyecto piloto tiene dos niveles de investigación. Por un lado, el de una moneda criptográfica mayorista, restringida a un grupo limitado de contrapartes financieras (mercado interbancario). Por el otro lado, el de una CBDC minorista, accesible para todo tipo de usuarios. Este último modelo permitiría reemplazar una parte del efectivo físico o suplementar el MO. El experimento o prueba de concepto ha mostrado que es posible construir una infraestructura digital de pago con una CBDC que no sólo preserve la privacidad de los usuarios, sino que simultáneamente las transacciones de mayor valor estén sujetas a las verificaciones obligatorias que prescribe la regulación europea de prevención del blanqueo de capitales. Ahora bien, los aspectos regulatorios de un hipotético Euro Digital son técnicamente complejos. Una nueva divisa diferente al euro fíat y al dinero bancario debería tener su propio esquema normativo y en particular, debería previamente despejarse cómo se anclaría a los depósitos de divisas del BCE y cómo mantendría una relación estable con el euro fíat, posiblemente de paridad o bajo un tipo de cambio estable.

Por otra parte, el Euro Digital contribuiría a culminar la eficacia de los sistemas de pago instantáneo existentes, en particular, el TIPS (TARGET Instant Payment Settlement), lanzado en noviembre de 2018. Esta red de pago instantáneo lanzada por el BCE proporciona una capa de liquidación para los bancos comerciales y si se adopta a gran escala, permitiría que las empresas y los particulares realicen transacciones entre ellos al instante y sin limitaciones de fin de semana u horario comercial. Según el BCE, el TIPS está diseñado para liquidar una carga regular de más de 43 millones de transacciones de pago instantáneo por día, y podría manejar hasta 2000 transacciones por segundo[9]. En esta fase preliminar, queda pendiente de confirmar si el TIPS y el Euro Digital podrán coexistir en el marco del Área Única de Pago en Euros (SEPA), y si su futura adopción comprometerá decisivamente o no la posición de los actores predominantes del mercado de pagos minoristas en Europa, cuyo control lo detentan empresas estadounidenses como Visa, MasterCard y PayPal.

El TIPS está diseñado para liquidar una carga regular de más de 43 millones de transacciones de pago instantáneo por día, y podría manejar hasta 2000 transacciones por segundo

También queda pendiente como afectará la irrupción de un Euro Digital al sector de las Bigtech/GAFA, que aspiran a ofrecer servicios financieros a los usuarios de sus plataformas (Google, Amazon, Facebook, Apple). Estos gigantes digitales cuentan ya con sistemas de comercio electrónico capaces de incorporar sus propios medios de pago

---

[7] Cabe mencionar que el evento de criptomonedas más grande a nivel mundial, "Consensus 2020", organizado por Coindesk y celebrado virtualmente en el pasado mes de mayo, contó con la participación de Yves Mersch, el principal funcionario del BCE como primer ponente (Keynote Speaker). (https://www.coindesk.com/events/consensus-2020). Puede leerse su discurso: "An ECB digital currency – a flight of fancy?" (11 de mayo de 2020) en: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html

[8] EUROchain se basa en intermediarios que tienen acceso a las cuentas del banco central y pueden recurrir a los saldos de reserva para proporcionar moneda digital al banco central a los usuarios. Los intermediarios procesarían transacciones en nombre de sus clientes. Su objetivo es buscar un equilibrio entre un cierto grado de privacidad en los pagos electrónicos y garantizar el cumplimiento de las normas destinadas a la prevención del blanqueo de capitales. En este sentido, la DLT no mostrará la identidad del usuario ni su historial de transacciones al banco central ni a los intermediarios que traten con el movimiento. Para profundizar sobre esta materia, véase el informe del BCE, "Exploring anonymity in central bank digital currencies", 4 de diciembre de 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

[9] Sobre este particular, véase, Panneta, F., "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis", The ECB Blog, 28 de abril de 2020. Este informe también menciona sistemas similares para liquidar transacciones bancarias a gran escala, denominadas Target2, así como Target2 Securities. Estos sistemas se están utilizando actualmente para liquidar transacciones financieras en Europa. (https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog200428~328d7ca065.en.html).

alternativos a la banca comercial y en un futuro próximo también pueden aspirar a detentar el poder de emisión y control de monedas virtuales estables con las que operar las transacciones dentro de sus marketplaces, con aplicaciones propias de pago a través de sus redes sociales y servicios de mensajería online. En este sentido, la regulación de las plataformas de servicio de cambio de moneda virtual por dinero fiduciario y de servicios de custodia de monedero electrónico (ewallets) es una materia que la UE tiene pendiente, porque la aproximación vigente se ha limitado casi estrictamente al campo de la prevención del fraude fiscal y del blanqueo de capitales. Sin embargo, constituye un sector tecnológico tan innovador que el enfoque europeo debería ser más audaz y menos reduccionista, porque indirectamente podría beneficiar a los Estados pero también a la banca comercial tradicional.

De momento, en el contexto europeo lo que ha trascendido es que el Banco de Francia, en asociación con el banco de inversión Société Générale, se encuentra desde enero haciendo experimentos relativos a un CBDC europeo. Según se dio a conocer, esta experimentación se realizó con infraestructura DLT/Blockchain, aunque dio a los operadores la flexibilidad de trabajar fuera de las limitaciones de esta tecnología[10]. Más recientemente, el Banco de Francia ha seleccionado ocho instituciones financieras como parte de una serie de pruebas para su próxima etapa de experimentos[11]. Entre los elegidos se encuentran Seba Bank, Societe Generale, ProsperUS, HSBC, Accenture, Euroclear, Iznes y LiquidShare, que desarrollarán proyectos que pondrán a prueba la idoneidad de la CBDC para resolver las transacciones de activos financieros[12].

En lo que respecta al Banco Central de los Países Bajos (DNB), también anunció el desarrollo de pruebas sobre el Euro Digital, sobre el que ha dicho que puede ser más programable que Bitcoin. A diferencia del Banco de Francia, la propuesta del DNB se está enfocando en la construcción de un sistema monetario público con el fin de que sea adoptado por el Eurosistema[13]. Diferente opinión ha expresado el Bundesbank alemán, que ha advertido de que un CBDC europeo podría desestabilizar los sistemas financieros europeos, aunque la Asociación de Bancos Alemanes sí ha abogado por una divisa digital programable[14].

Por su parte, cabe destacar que la Asociación Bancaria Italiana (ABI), compuesta por 700 entidades de crédito, anunció en el mes de julio que sus bancos están dispuestos a poner a prueba el Euro Digital, respaldado por el BCE. El grupo que lidera esta iniciativa compartió 10 puntos sobre las

---

[10] Como parte del experimento, Societe Generale emitió bonos por 40 millones de euros, recibiendo el pago en forma de euro digital (CBDC), emitido por el Banco de Francia. Mediante la inclusión de contratos inteligentes, se consiguió un ahorro de costes y de tiempo. Francia se ha centrado principalmente la solución mayorista antes de considerar la implementación de una CBDC minorista.

[11] Banque de France, "Avancement de la démarche d'expérimentations de monnaie digitale de banque centrale lancée par la Banque de France", 20 de mayo de 2020. https://www.banque-france.fr/sites/default/files/medias/documents/experimentation_mdbc_mai_2020.pdf.

[12] Banque de France, "Liste des candidatures retenues pour les expérimentations de monnaie digitale de banque centrale (MDBC)", 20 de julio de 2020. (https://www.banque-france.fr/communique-de-presse/liste-des-candidatures-retenues-pour-les-experimentations-de-monnaie-digitale-de-banque-centrale).

[13] DNP, "Central Bank Digital Currency: Objectives, preconditions and design choices", 2020. En la noticia del DNBulletin: "Digital currency issued by central banks can protect public interests in payment systems" se afirma: "Una CBDC puede diseñarse como cuentas que las personas físicas y jurídicas tienen con un banco central. Al igual que los billetes en circulación, la CBDC estaría en el balance del banco central. Las empresas privadas podrían desarrollar aplicaciones fáciles de usar para que los hogares y las empresas realicen pagos en CBDC. Las tecnologías específicas que fueron pioneras anteriormente para algunos criptos podrían usarse en el ecosistema CBDC para reducir los costes de transacción para ciudadanos y empresas. El volumen de CBDC en circulación podría controlarse mediante los intereses pagados sobre los saldos y estableciendo límites. La tasa de interés de mercado podría aplicarse a una cantidad básica específica de CBDC mantenida por cada ciudadano o empresa, y una escala gradualmente creciente de tasas de penalización podría aplicarse a los saldos en exceso. Esto haría poco atractivo mantener grandes cantidades en CBDC. También se podrían considerar límites absolutos, lo que evitaría un movimiento masivo a CBDC durante las crisis financieras". Por otra parte, el documento del DNB también destaca que los porcentajes relativos de transacciones realizadas con efectivo y con medios electrónicos han cambiado desde 2010. Mientras que los consumidores holandeses pagaron el 35% de sus transacciones electrónicamente y el 65% en efectivo hace una década, las cifras se situaban en el 32% por efectivo y 68% electrónico en 2019. (https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2020/dnb388309.jsp).

[14] https://www.bundesbank.de/en/press/interviews/weidmann-calls-for-a-hard-line-on-libra-821340

La posición de la asociación bancaria alemana puede encontrarse en Bundesverband deutscher Banken, "Following the debate on Facebook's "Libra" currency, German banks say: The economy needs a programmable digital euro!", 30 de octubre de 2019. https://bankenverband.de/media/files/Paper_programmable-digital-euro.pdf. Asimismo, el pasado 23 de julio de 2020, el Consejo FinTech del Ministerio Federal de Finanzas de Alemania publicó un informe sobre el euro digital programable. En dicho informe se explican las razones por las cuales el euro digital programable sería beneficioso para el sector bancario y para los usuarios finales, por el aumento de la eficiencia en los pagos transfronterizos, la automatización, la integración de la entrega versus el pago en una plataforma y la habilitación de micropagos. También presenta diferentes enfoques sobre cómo podría emitirse e implementarse el euro digital programable. FinTechRat beim Bundesministerium der Finanzen, "Der digitale,programmierbare Euro", 2020.

consideraciones que conlleva esta propuesta de CBDC europea[15]. La cuestión prioritaria, a juicio de la ABI, es preservar la estabilidad monetaria y el pleno cumplimiento del marco regulatorio europeo. Por tanto, el marco jurídico de una CBDC del BCE habría de ser, según la ABI, plenamente compatible con las regulaciones de la Unión Europea. Por esta razón, la clave sería generar confianza en sus usuarios, es decir, crear valor añadido sobre el resto de los criptoactivos del mercado con función de pago, pero también respecto a las hipotéticas monedas digitales lideradas por los gigantes de Internet que se introduzcan próximamente en el sector Fintech[16].

La cuestión prioritaria, a juicio de la ABI, es preservar la estabilidad monetaria y el pleno cumplimiento del marco regulatorio europeo

A este respecto, la aparición de una CBDC en el sistema bancario europeo supondría mejorar la competitividad de la banca ante las disrupciones de las grandes empresas tecnológicas, incorporando transacciones programables P2P y M2M con supervisión de una autoridad oficial. En el caso de una CBDC europea, gobernada por el BCE, representa sin duda un valor añadido que las criptomonedas descentralizadas no pueden ofrecer ni tampoco los proyectos privados de stablecoins como Libra. Por tanto, tal y como pone de manifiesto la propuesta italiana, una CBDC supone la capacidad de administrar el riesgo de tipo de cambio y de tasa de interés porque las facultades programables de la moneda virtual están en manos de una autoridad central y no dependen de comunidades virtuales anónimas y opacas[17]. Por todo ello, como afirma la ABI, una moneda digital programable y de curso legal representa una innovación en el campo financiero que sería capaz de revolucionar profundamente el dinero y el intercambio, representando una transformación que podría aportar un valor potencial muy significativo, particularmente en términos de eficiencia de los procesos operativos y de gestión, pero también en seguridad jurídica.

3. INTERROGANTES SOBRE EL EURO DIGITAL A DESPEJAR PRÓXIMAMENTE

La introducción de una CBDC europea (Euro Digital) presenta en estos momentos múltiples desafíos, tanto tecnológicos como políticos y regulatorios. Si la moneda virtual europea va a ser una nueva reserva dentro del balance del BCE, cabe la opción de que los usuarios, esto es, los ciudadanos europeos, pudiesen solicitar la apertura de cuentas y depósitos directamente en el banco central, reduciendo así el rol de la banca comercial como intermediario. Esta posibilidad teórica supondría una extraordinaria transformación del modelo bancario europeo. De hecho, es la vía que está emprendiendo el Banco Popular de China con el Yuan Digital, licitando las licencias para los proveedores de monedero electrónico, directamente vinculados a las cuentas de la banca central. Estas licencias se van a asignar mayoritariamente a Wechat Pay y AliPay, que son los sistemas de pago de los gigantes tecnológicos chinos Tencent y Alibaba, respectivamente.

De momento, la razón principal por la que en la UE no se plantea que el BCE ofrezca directamente acceso a sus fondos de CBDC a sus ciudadanos particulares -a pesar de que la tecnología para hacerlo está disponible-, es sencillamente porque realizar esta operación podría suponer graves con-

---

[15] "Una moneda digital programable representa una innovación en el campo financiero capaz de revolucionar profundamente el dinero (…) De ahí la importancia de dedicar atención y energía para desarrollar, rápidamente y con la colaboración de todos los actores del ecosistema, herramientas útiles en primer lugar para el desarrollo de la zona del euro". (https://www.abi.it/Pagine/news/MonetaDigitale.aspx).

[16] En lo que respecta a su dimensión tecnológica, la ABI menciona el proyecto Spunta, iniciativa del Laboratorio ABI, que consiste en integrar la tecnología de la cadena de bloques (DLT/Blockchain) en el procesamiento de información interbancaria. La novedosa propuesta italiana es una demostración de que la introducción de un CBDC conduce a innovaciones digitales dentro del sistema bancario, facilitando su modernización y digitalización, aspecto clave para no perder el tren del desarrollo tecnológico en Europa, que hoy por hoy lideran las grandes empresas tecnológicas estadounidenses. (https://www.r3.com/wp-content/uploads/2019/04/Spunt_CS_R32018.pdf).

[17] En este sentido, resulta de interés el informe del MIT, "Redesigning digital money: What can we learn from a decade of cryptocurrencies?", Digital Currency Initiative, MIT Media Lab, 22 de enero de 2020, en el que se examinan las principales aportaciones de la industria DLT/Blockchain hasta el momento, incluyendo los protocolos de consenso de cadenas de bloques descentralizados, las transacciones atómicas en cadena como ejemplo de dinero programable y los métodos de privacidad basados en blockchain.

secuencias para la banca comercial europea. No obstante, la hipótesis de que los particulares pudiesen convertir sus depósitos bancarios en una moneda digital centralizada con una ecuación de canje 1:1 encontraría sin duda un gran atractivo, máxime en una coyuntura de comisiones bancarias al alza y de tipos de interés nulos o incluso negativos. Sin embargo, una posible fuga de depósitos desde la banca comercial al BCE podría magnificar los efectos de la crisis actual y poner en mayor peligro la sostenibilidad de las entidades de crédito[18]. Una CBDC convertible a la divisa fiduciaria bancaria podría, en efecto, provocar un desplazamiento de depósitos bancarios arrastrando graves consecuencias para toda la estructura del sistema financiero. Esto en la práctica dificultaría la capacidad del BCE para cumplir su misión de transmitir su política monetaria a la economía real.

Además, en el supuesto de que el BCE tomara depósitos minoristas, quedaría por resolver si también se reserva la facultad de otorgar préstamos. Esto supondría introducirse en líneas comerciales orientadas al cliente, además de asumir la carga del cumplimiento normativo en materia de prevención del blanqueo de capitales, protección de consumidores y confidencialidad. Podría argumentarse a favor de otorgar esta facultad al banco central que esta medida ayudaría a la inclusión financiera, además de reforzar la soberanía monetaria, ya que la desintermediación podría hacer más seguro y equitativo al sistema financiero. En sentido contrario, una CBDC a nivel minorista podría crear una concentración desproporcionada de poder en el banco central, lo que en determinados contextos podría generar efectos muy adversos en el sistema financiero, pero fundamentalmente en el modelo de negocio de la banca comercial, puesto que a día de hoy los depósitos minoristas representan fuentes de financiación baratas y de alta calidad para los bancos comerciales. Por tanto, si una CBDC se implantara y quitara los depósitos, dejaría la financiación más cara y dependiente de los mercados mayoristas, cortando a su vez el vínculo con los clientes. Si las cuentas corrientes y depósitos bancarios perdiesen importancia por la disrupción de una CBDC, los bancos comerciales podrían convertirse en proveedores de capital de balance solamente y esto dejaría más reducidos sus ingresos por comisiones.

Finalmente, en torno al Euro Digital tampoco se ha esclarecido sí tendría una remuneración, y si ésta, en caso de introducirse, se establecería con unos tipos por debajo de los de mercado. El BCE ha abordado tímidamente esta cuestión, planteando un sistema de CBDC escalonado con dos tasas de interés diferentes. Si se excediese un cierto umbral de CBDC en la cuenta del banco central, el excedente se remuneraría con tasas de interés cero o incluso negativas[19]. Ahora bien, este planteamiento no es nuevo habida cuenta de que, desde el 12 de septiembre de 2019, el Consejo del Banco Central Europeo precisamente ha decidido introducir un sistema de dos niveles para los intereses sobre saldos de reservas mantenidas que exceden el objetivo de reserva mínima (objetivo de MR) (reservas excedentes). Esto en la práctica viene a establecer una exención a los bancos comerciales de pagar intereses sobre una cantidad de reservas mínimas que tienen que mantener con el banco central para cumplir con los requisitos de liquidez. Actualmente, el exceso de reservas se remunera negativamente -0.5%[20]. Por tanto, bajo este planteamiento lo que se buscaría es que la tenencia de la CBDC europea por encima de un límite nunca se remunerara positivamente, es decir, que el mantenimiento de un excedente de Euro Digital no supondría ningún tipo de inversión, protegiendo así a la banca comercial de un posible corralito. Básicamente, con esta medida se evitaría que

---

[18] En este sentido resulta de interés la entrevista a Jens Weidmann, presidente del Bundesbank alemán, en el diario alemán Handelsblatt, en la que argumenta que la introducción de una CBDC podría conducir a un corralito bancario, porque una considerable liquidez del sector bancario se trasladaría al banco central, lo que podría resultar en una falta de financiación para el sector de la banca comercial. "Los depositantes asustados podrían desencadenar una crisis de liquidez en el sistema bancario al retirar su dinero a una cuenta segura en el banco central". (https://www.handelsblatt.com/finanzen/geldpolitik/geldpolitik-bundesbank-praesident-weidmann-warnt-vor-einfuehrung-eines-digitalen-euros/25362418.html?nlayer=Newsticker_1985586&ticket=ST-240647-XrK6buG47TDnt4SjyFPN-ap2).

[19] Esta idea ha sido formulada por el Director General de Infraestructura de Mercado en el BCE, Ulrich Bindseil, expuesta en su informe: "Tiered CBDC and the financial system", ECB Working Paper Series, Nº 2351, enero de 2020.

[20] Vid. Reglamento (CE) Nº 1745/2003 del BCE, de 12 de septiembre de 2003, relativo a la aplicación de las reservas mínimas (BCE/2003/9) y Decisión (UE) 2019/1743 del BCE de 15 de octubre de 2019, relativa a la remuneración de las tenencias de exceso de reservas y de determinados depósitos (refundición) (BCE/2019/31). (https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.mp190912~08de50b4d2.es.html).

los usuarios del Euro Digital pudieran usar la CBDC como una reserva de valor, cambiando sus ahorros privados depositados en los bancos comerciales por su cuenta de CBDC en el BCE.

Todo lo anteriormente comentado sobre las dificultades de una CBDC europea viene en cierto modo a dar la razón a aquellos autores que sostienen que la denominada Unión Monetaria no es tal, ya que en realidad solo funciona como una unión de efectivo (cash union), en la que el efectivo físico (las monedas y billetes de euros) que usan los ciudadanos europeos son los mismos, esto es, tienen el mismo valor en los distintos países, pero no así los euros que están depositados en los bancos privados de cada Estado miembro, que no tienen el mismo valor. Por este motivo, para encaminar al Espacio Económico Europeo hacia una verdadera Unión Monetaria y Bancaria, el lanzamiento de un Euro Digital emitido por el BCE sería un paso fundamental[21].

4. CONCLUSIÓN

El auge del sector criptomonetario ha provocado la reacción de las autoridades bancarias y financieras internacionales. Mientras que las criptomonedas tienen una estructura descentralizada y de momento sólo están actuando como reserva de valor ante la devaluación del dinero fíat, los proyectos de los bancos centrales presentan a sus CBDC como una divisa electrónica y centralizada, un activo líquido y seguro que tendría un triple uso: efectivo, depósito de valor y medio de pago.
El BCE se encuentra actualmente inmerso en su propio proyecto de CBDC. Francia y los Países Bajos abanderan los avances entre los Estados Miembros. Los primeros desarrollos evidencian una apuesta decidida de la Unión Europea por la creación de una moneda digital de banco central que, de implantarse, revolucionará el sistema financiero mundial. En este sentido, la Unión Europea tiene ante sí la oportunidad de impulsar la Unión Monetaria y Bancaria, situándose a la vanguardia de la revolución digital financiera, en el que la CBDC quedaría integrada dentro de la nueva plataforma de pagos paneuropea, de base criptográfica y programable.

REFERENCIAS:

BCE, "Exploring anonymity in central bank digital currencies", 4 December 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Bindseil, U., "Tiered CBDC and the financial system", ECB Working Paper Series, Nº 2351, January 2020.

BIS, Impending arrival – a sequel to the survey on central bank digital currency, BIS Papers, Nº 107, 2020.https://www.bis.org/publ/bppdf/bispap107.pdf

Brunnermeier, M.K., Landeau, J.P. y James, H., "The Digitalization of Money", University of Princeton, August 2019. (https://scholar.princeton.edu/sites/default/files/markus/files/02c_digitalmoney.pdf).

Bundesverband deutscher Banken, "Following the debate on Facebook's "Libra" currency, German banks say: The economy needs a programmable digital euro!", 30 October 2019. https://bankenverband.de/media/files/Paper_programmable-digital-euro.pdf

DNP, "Central Bank Digital Currency: Objectives, preconditions and design choices", 2020. (https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2020/dnb388309.jsp

FinTechRat beim Bundesministerium der Finanzen, "Der digitale,programmierbare Euro", 2020. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Finanzmarktpolitik/2020-07-08-fintechrat-digitaler-euro.pdf?__blob=publicationFile&v=3

Mayer, Th., "A digital euro to save EMU", Vox EU-CEPR, 6 November 2019 (https://voxeu.org/article/digital-euro-save-emu).

Mersch, Y., "An ECB digital currency – a flight of fancy?", 11 March 2020 (https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html).

MIT, "Redesigning digital money: What can we learn from a decade of cryptocurrencies?", Digital Currency Initiative, MIT Media Lab, 22 January 2022.

Panneta, F., "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis", The ECB Blog, 28 Abril 2020. (https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog200428~328d7ca065.en.html).

The Wall Street Journal, "Former Regulator Known as 'Crypto Dad' to Launch Digital-Dollar Think Tank", 16 January 2020.

The Wall Street Journal, "We Sent a Man to the Moon. We Can Send the Dollar to Cyberspace", 15 October 2019.

WEF, "Central Bank Digital Currency Policy-Maker Toolkit", White Paper, 22 January 2020. https://www.weforum.org/whitepapers/central-bank-digital-currency-policy-maker-toolkit

[21] Esta tesis puede encontrarse en: Mayer, Th., "A digital euro to save EMU", Vox EU-CEPR, 6 de noviembre de 2019 (https://voxeu.org/article/digital-euro-save-emu).

Digital Euro: context and regulatory perspectives

Pablo Sanz Bayón
ICADE Commercial Law Professor

1. INTRODUCTION TO CENTRAL BANK DIGITAL CURRENCIES (CBDC)

The ecosystem of the digital economy has given rise in recent years to the proliferation of a multiplicity of new means of payment, intermediaries and platforms. Among the actors that are beginning to play a prominent role is the virtual currencies sector, and specifically, within it, that of cryptocurrencies, with Bitcoin standing out among them. As is known, these digital assets or tokens are characterized by using a cybernetic and cryptographic infrastructure of distributed ledger (DLT / Blockchain), which involves the decentralization and anonymity of economic relations and payments (P2P). As a consequence of the financial innovation that this digital technology and its actors are generating, monetary and banking systems around the world have begun to react to this challenge[1].The digitization of alternative forms of money, that is, the appearance of crypto assets with a payment function, is indeed a frontal challenge to traditional monetary policy. In addition, the rise of this computer innovation has been contemporary and has been fed back by reason of the global economic crisis, unprecedented in modern history. A crisis that originated in 2008 that has tried to be neutralized by a policy of expansion of the money supply, extraordinarily strengthened in the first

half of 2020, as a measure to stimulate demand. This situation has led the financial system to very low, zero or even negative interest rates, which in turn has been awakening the attractiveness of investors for more profitable assets, such as cryptocurrencies.

The evolution of these events has led in recent months to the development of research on central bank virtual currencies, the so-called Central Bank Digital Currencies (CBDC), in which the conservation of the State's monetary sovereignty is at the center of the debate[2]. What is proposed as a hypothetical scenario could give rise to a true systemic risk if the trend is not corrected by the authorities and a majority of the world population is migrating and shifting their fiat money deposits towards alternative digital forms, such as cryptocurrencies. decentralized or corporate virtual currencies (stablecoins like Libra, from the consortium led by Facebook).

The emergence of electronic commerce ecosystems, with their respective global marketplaces and gigantic user communities, with mobile applications operated by a multitude of payment, exchange and custody service providers for electronic wallets would displace commercial banks from the market and place the monetary traffic outside the control perimeter of the supervisory authorities. In this context, the international financial architecture and its postulates of stability could be compromised if a coordinated response is not proposed at the supranational and intergovernmental level on cryptocurrencies, going beyond fiscal aspects and the prevention of money laundering. Therefore, a response to this challenge is beginning to crystallize in institutional projects on CBDC[3]. The central bank would be its issuer and would be an essential element in the total digitalization of the payments market, with the intention of gradually replacing physical cash[4]. The paradigm shift

---

[1] For a preliminary study on the challenges of digitizing money, see: Brunnermeier, M.K., Landeau, J.P. y James, H., "The Digitalization of Money", University of Princeton, August 2019 (https://scholar.princeton.edu/sites/default/files/markus/files/02c_digitalmoney.pdf).

[2] Outside the DLT / Blockchain technology environment, there are alternatives, such as the FedNow service in the US, which focuses on improving the speed of payments. https://www.frbservices.org/financial-services/fednow/index.html

[3] Last January, the World Economic Forum, together with some of the world's leading central banks, established a toolkit for policy-making on CBDCs. See in this regard: WEF White Paper: "Central Bank Digital Currency Policy-Maker Toolkit", 22 January 2020.

[4] The director of the BIS, Agustín Carstens, acknowledged last March that the main reason for the acceleration of these projects is undoubtedly due to the emergence of cryptocurrencies, and particularly, to stablecoin projects, such as Libra, promoted by Facebook . Stablecoins have been scrutinized in detail by a G7 working group. What is behind the impulse to the CBDC is to safeguard monetary sovereignty in the face of the emergence of these digital assets in the digital economy, accompanied by multiple payment and exchange systems.

could be radical because it would mean separating the regulation of money from the regulation of the financial system.

The Bank for International Settlements (BIS), in a survey this year, has said that more than 80% of the 66 central banks consulted have acknowledged that they are working on CBDC projects. In answering about their main motivations, central banks show some differences, however. Banks in emerging countries understand CBDCs as a mechanism aimed, above all, at improving the efficiency and security of national payments, and also to promote financial inclusion. However, advanced economies justify their investigations at CBDC primarily on security of payments and financial stability[5].

The states that are taking the lead are those emerging that have more vulnerabilities in terms of cash control, with broad social layers excluded from the financial system, with difficulties in preventing money laundering or that can afford, due to their idiosyncrasies, to promote quickly digitize your financial services. However, the power and influence of the largest central banks will be the factor that will surely determine the definitive development of CBDCs in the near future.

The European Central Bank (ECB) is among them, but not at the level of its Chinese counterpart, the People's Bank of China, which has already developed and is testing a pilot project on the Digital Yuan (DC / EP), which It will be pegged 1:1 to the national currency, the RenMinBi (RMB). By contrast, in the US, the Digital Dollar project, promoted by former CFTC president Christopher Giancarlo but outside the Federal Reserve, is still in a very embryonic phase, after having rejected its legal introduction through the programs. of stimuli against the coronavirus crisis[6].

The greatest challenge for banking and monetary regulators is that the CBDC is stable, that is, that its offer is managed and provides confidence to serve as a means of payment with the capacity to progressively replace physical cash. That is why the launch of a CBDC not only implies the emergence of a more technologically advanced means of payment, but also that the diversity of regulatory approaches can have different effects on the monetary policy of a central bank and with respect to guarantee financial stability. The CBDCs come, in this sense, to neutralize the rise of cryptocurrencies, whose capitalization and dissemination begins to be more and more considerable, although their utility for the moment is not as a means of payment but fundamentally as a store of value.

2. THE ECB DIGITAL EURO PROJECT

As the ECB itself has recognized, its motivation for the Digital Euro is to be prepared at a technological and regulatory level for when this dis-

[5] Vid. BIS," Impending arrival – a sequel to the survey on central bank digital currency", BIS Papers, Nº 107, 2020 (https://www.bis.org/publ/bppdf/bispap107.pdf).

[6] The debate on a CBDC in the US was encouraged over a draft of a stimulus bill to face the economic effects of the pandemic. This bill suggested the use of a digital dollar to facilitate the distribution of payments in a fast and contactless way. In the end, the idea was dismissed and disappeared from the final draft of the bill. About the Digital Dollar project, see the articles in The Wall Street Journal, "We Sent a Man to the Moon. We Can Send the Dollar to Cyberspace", 15 October 2019, and "Former Regulator

ruption occurs completely[7]. Hence, the ECB has delegated to 5 European central banks, in collaboration with the BIS, the study of the viability of their CBDC through a proof of concept project "EuroChain" on the Corda platform, from R3 and with the support of Accenture[8]. This pilot project has two levels of research. On the one hand, that of a wholesale crypto currency, restricted to a limited group of financial counterparties (interbank market). On the other hand, that of a retail CBDC, accessible to all types of users. This last model would allow to replace a part of the physical cash or to supplement the MO. The experiment or proof of concept has shown that it is possible to build a digital payment infrastructure with a CBDC that not only preserves the privacy of users, but simultaneously the higher value transactions are subject to the mandatory verifications prescribed by the European regulation of prevention of money laundering. However, the regulatory aspects of a hypothetical Digital Euro are technically complex. A new currency other than the fiat euro and bank money should have its own regulatory scheme and in particular, it should be previously clarified how it would be anchored to the ECB's currency deposits and how it would maintain a stable relationship with the fiat euro, possibly at parity or low a stable exchange rate.

On the other hand, the Digital Euro would contribute to culminating the effectiveness of existing instant payment systems, in particular the TIPS (TARGET Instant Payment Settlement), launched in November 2018. This instant payment network launched by the ECB provides a layer of settlement for commercial banks and if adopted on a large scale, would allow businesses and individuals to transact with each other instantly and without weekend or business hour limitations. According to the ECB, the TIPS is designed to settle a regular load of more than 43 million instant payment transactions per day,

The TIPS is designed to settle a regular load of more than 43 million instant payment transactions per day, and could handle up to 2,000 transactions per second

and could handle up to 2,000 transactions per second[9]. In this preliminary phase, it remains to be confirmed whether the TIPS and the Digital Euro can coexist within the framework of the Single Payment Area in Euros (SEPA), and whether their future adoption will decisively compromise or not the position of the predominant players in the market for retail payments in Europe, controlled by US companies such as Visa, MasterCard and PayPal.

It is also pending how the irruption of a Digital Euro will affect the Bigtech / GAFA sector, which aspire to offer financial services to the users of their platforms (Google, Amazon, Facebook, Apple). These digital giants already have electronic commerce systems capable of incorporating their own alternative means of payment to commercial banking and in the near future they may also aspire to hold the power to issue and control stable virtual currencies with which to operate transactions within of its marketplaces, with its own payment applications through its social networks and online

[7] It is worth mentioning that the largest cryptocurrency event in the world, "Consensus 2020", organized by Coindesk and held virtually last May, had the participation of Yves Mersch, the main official of the ECB as Keynote Speaker. (https://www.coindesk.com/events/consensus-2020). His speech can be read: "An ECB digital currency – a flight of fancy?" (11 May 2020): https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html

[8] EUROchain relies on intermediaries who have access to central bank accounts and can draw on reserve balances to provide digital currency to the central bank to users. The intermediaries would process transactions on behalf of their clients. Its objective is to find a balance between a certain degree of privacy in electronic payments and guarantee compliance with the regulations aimed at the prevention of money laundering. In this sense, the DLT will not show the identity of the user or his transaction history to the central bank or to the intermediaries that deal with the movement. For further information on this matter, see the ECB report, "Exploring anonymity in central bank digital currencies", 4 December 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

[9] See Panneta, F., "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis", The ECB Blog, 28 Abril 2020. This report also mentions similar systems for settling large-scale bank transactions, called Target2, as well as Target2 Securities. These systems are currently being used to settle financial transactions in Europe. (https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog200428~328d7ca065.en.html).

messaging services. In this sense, the regulation of virtual currency exchange service platforms for fiduciary money and electronic wallet custody services (ewallets) is a matter that the EU has pending, because the current approach has been almost strictly limited to the field of the prevention of tax fraud and money laundering. However, it is such an innovative technology sector that the European approach should be bolder and less reductionist, because it could indirectly benefit states but also traditional commercial banks.

For the moment, in the European context, what has transpired is that the Bank of France, in association with the investment bank Société Générale, has been conducting experiments on a European CBDC since January. This experimentation was reportedly done with DLT / Blockchain infrastructure, although it gave operators the flexibility to work outside the limitations of this technology[10]. More recently, the Bank of France has selected eight financial institutions as part of a series of tests for its next stage of experiments[11]. Among those chosen are Seba Bank, Societe Generale, ProsperUS, HSBC, Accenture, Euroclear, Iznes and LiquidShare, which will develop projects that will test the suitability of the CBDC to resolve financial asset transactions[12].

As far as the Central Bank of the Netherlands (DNB) is concerned, it also announced the development of tests on the Digital Euro, which it has said may be more programmable than Bitcoin. Unlike the Bank of France, the DNB proposal is focusing on the construction of a public monetary system in order for it to be adopted by the Eurosystem[13]. Different opinion has been expressed by the German Bundesbank, which has warned that a European CBDC could destabilize European financial systems, although the Association of German Banks has advocated for a programmable digital currency[14].

---

[10] As part of the experiment, Sócieté Générale issued bonds for 40 million euros, receiving payment in the form of a digital euro (CBDC), issued by the Bank of France. By including smart contracts, cost and time savings were achieved. France has primarily focused on the wholesale solution before considering implementing a retail CBDC.

[11] Banque de France, "Avancement de la démarche d'expérimentations de monnaie digitale de banque centrale lancée par la Banque de France", 20 May 2020. https://www.banque-france.fr/sites/default/files/medias/documents/experimentation_mdbc_mai_2020.pdf.

[12] Banque de France, "Liste des candidatures retenues pour les expérimentations de monnaie digitale de banque centrale (MDBC)", 20 July 2020. (https://www.banque-france.fr/communique-de-presse/liste-des-candidatures-retenues-pour-les-experimentations-de-monnaie-digitale-de-banque-centrale).

[13] DNP, "Central Bank Digital Currency: Objectives, preconditions and design choices", 2020. (https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2020/dnb388309.jsp

[14] https://www.bundesbank.de/en/press/interviews/weidmann-calls-for-a-hard-line-on-libra-821340

The position of the German banking association can be found at Bundesverband deutscher Banken, "Following the debate on Facebook's "Libra" currency, German banks say: The economy needs a programmable digital euro!", 30 October 2019. https://bankenverband.de/media/files/Paper_programmable-digital-euro.pdf

Also, on July 23, 2020, the FinTech Council of the Federal Ministry of Finance of Germany published a report on the programmable digital euro. This report explains the reasons why the programmable digital euro would be beneficial for the banking sector and for end users, by increasing efficiency in cross-border payments, automation, integration of delivery versus payment in a platform and enabling micropayments. It also presents different approaches to how the programmable digital euro could be issued and implemented. FinTechRat beim Bundesministerium der Finanzen, "Der digitale,programmierbare Euro", 2020. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Finanzmarktpolitik/2020-07-08-fintechrat-digitaler-euro.pdf?__blob=publicationFile&v=3

For its part, it should be noted that the Italian Banking Association (ABI), made up of 700 credit institutions, announced in July that its banks are willing to test the Digital Euro, backed by the ECB. The group leading this initiative shared 10 points about the considerations involved in this European CBDC proposal[15]. The priority issue, in the opinion of the ABI, is to preserve monetary stability and full compliance with the European regulatory framework. Therefore, the legal framework of an ECB CBDC should be, according to the ABI, fully compatible with the regulations of the European Union. For this reason, the key would be to generate trust in its users, that is, to create added value over the rest of the crypto assets on the market with a payment function, but also with respect to the hypothetical digital currencies led by the Internet giants that will be introduced soon. in the Fintech sector[16].

The priority issue, in the opinion of the ABI, is to preserve monetary stability and full compliance with the European regulatory framework

In this regard, the appearance of a CBDC in the European banking system would mean improving the competitiveness of banks in the face of disruptions from large technology companies, incorporating programmable P2P and M2M transactions supervised by an official authority. In the case of a European CBDC, governed by the ECB, it certainly represents an added value that decentralized cryptocurrencies cannot offer and neither can private stablecoin projects like Libra. Therefore, as the Italian proposal shows, a CBDC assumes the ability to manage exchange rate and interest rate risk because the programmable powers of the virtual currency are in the hands of a central authority and do not depend on anonymous and opaque virtual communities[17]. Therefore, as stated by the ABI, a programmable and legal tender digital currency represents an innovation in the financial field that would be capable of profoundly revolutionizing money and exchange, representing a transformation that could bring a very significant potential value, particularly in terms of efficiency of operational and management processes, but also of legal certainty.

Therefore, as stated by the ABI, a programmable and legal tender digital currency represents an innovation in the financial field that would be capable of profoundly revolutionizing money and exchange, representing a transformation that could bring a very significant potential value, particularly in terms of efficiency of operational and management processes, but also of legal certainty.

3. QUESTIONS ABOUT THE DIGITAL EURO TO CLEAR SOON

The introduction of a European CBDC (Digital Euro) currently presents multiple challenges, both technological, political and regulatory. If the European virtual currency is going to be a new reserve within the balance sheet of the ECB, there is the option that users, that is, European citizens, could request the opening of accounts and deposits directly with the central bank, thus reducing the role commercial banking as an intermediary. This theoretical possibility would mean an extraordinary transformation of the European banking model. In fact, it is the path that the People's Bank of China is taking with the Digital Yuan,

[15] https://www.abi.it/Pagine/news/MonetaDigitale.aspx

[16] Regarding its technological dimension, the ABI mentions the Spunta project, an initiative of the ABI Laboratory, which consists of integrating blockchain technology (DLT / Blockchain) in interbank information processing. The novel Italian proposal is a demonstration that the introduction of a CBDC leads to digital innovations within the banking system, facilitating its modernization and digitization, a key aspect to not miss the train of technological development in Europe, which today is led by large companies American technology companies. (https://www.r3.com/wp-content/uploads/2019/04/Spunt_CS_R32018.pdf).

[17] See: MIT, "Redesigning digital money: What can we learn from a decade of cryptocurrencies?", Digital Currency Initiative, MIT Media Lab, 22 January 2020. This report examines the main contributions of the DLT / Blockchain industry so far, including decentralized blockchain consensus protocols, atomic transactions on chain as an example of programmable money, and blockchain-based privacy methods.

bidding for licenses for electronic wallet providers, directly linked to central bank accounts. These licenses will be assigned mostly to Wechat Pay and AliPay, which are the payment systems of Chinese technology giants Tencent and Alibaba, respectively.

At the moment, the main reason why the EU does not propose that the ECB offers direct access to its CBDC funds to its private citizens - despite the fact that the technology to do so is available - is simply because carrying out this operation could have serious consequences for European commercial banks. However, the hypothesis that individuals could convert their bank deposits into a centralized digital currency with a 1:1 exchange ratio would undoubtedly find great appeal, especially in a situation of rising bank commissions and zero or zero interest rates. even negative. However, a possible leakage of deposits from commercial banks to the ECB could magnify the effects of the current crisis and further jeopardize the sustainability of credit institutions[18]. A CBDC convertible to the bank fiat currency could, in effect, cause a displacement of bank deposits with serious consequences for the entire structure of the financial system. This in practice would hamper the ECB's ability to fulfill its mission of transmitting its monetary policy to the real economy.

Furthermore, in the event that the ECB took retail deposits, it remains to be resolved whether it also reserves the power to grant loans. This would mean entering into customer-oriented commercial lines, in addition to assuming the burden of regulatory compliance in the area of prevention of money laundering, consumer protection and confidentiality. It could be argued in favor of granting this power to the central bank that this measure would help financial inclusion, in addition to strengthening monetary sovereignty, since disintermediation could make the financial system safer and more equitable. On the contrary, a CBDC at the retail level could create a disproportionate concentration of power in the central bank, which in certain contexts could have very adverse effects on the financial system, but fundamentally on the business model of commercial banking, since Today, retail deposits represent inexpensive, high-quality sources of finance for commercial banks. Therefore, if a CBDC were to set up and remove deposits, it would make financing more expensive and dependent on wholesale markets, in turn cutting off the link with customers. If checking accounts and bank deposits were to lose importance due to the disruption of a CBDC, commercial banks could become providers of balance sheet capital only, further reducing their fee income.

Finally, regarding the Digital Euro it has not been clarified whether it would have a remuneration, and if this, if introduced, would be established with rates below market rates. The ECB has timidly approached this issue, raising a tiered CBDC system with two different interest rates. If a certain CBDC threshold is exceeded in the central bank account, the surplus would be remunerated at zero or even negative interest rates[19]. However, this approach is not new given that, since 12 September 2019, the Council of the European Central Bank has precisely decided to introduce a two-tier system for interest on balances of reserves held that exceed the reserve target. minimum (MR target) (surplus reserves).
This in practice establishes an exemption for commercial banks from paying interest on a minimum amount of reserves that they have to maintain with the central bank to meet liquidity requirements. Currently, excess reserves are negatively remunerated -0.5%[20]. Therefore, under this approach, what would be sought is that the holding of the European CBDC above a limit will never be positively remunerated, that is, that the maintenance of a surplus of Euro Digital would not involve any type of investment, thus protecting the commercial bank of a possible corrali-

---

[18] In this sense, the interview with Jens Weidmann, president of the German Bundesbank, in the German newspaper Handelsblatt, in which he argues that the introduction of a CBDC could lead to a banking corralito, because a considerable liquidity of the banking sector would be transferred to the central bank, which could result in a lack of funding for the commercial banking sector. "Scared depositors could trigger a liquidity crisis in the banking system by withdrawing their money to a secure account at the central bank." (https://www.handelsblatt.com/finanzen/geldpolitik/geldpolitik-bundesbank-praesident-weidmann-warnt-vor-einfuehrung-eines-digitalen-euros/25362418.html?nlayer=Newsticker_1985586&ticket=ST-240647-XrK6buG47TDnt4SjyFPN-ap2).

[19] Ulrich Bindseil, "Tiered CBDC and the financial system", ECB Working Paper Series, Nº 2351, January 2020.

[20] https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.mp190912~08de50b4d2.es.html

to. Basically, this measure would prevent Digital Euro users from being able to use the CBDC as a store of value, exchanging their private savings deposited in commercial banks for their CBDC account at the ECB.

Everything previously commented on the difficulties of a European CBDC comes in a way to agree with those authors who argue that the so-called Monetary Union is not such, since in reality it only functions as a cash union, in that the physical cash (the euro coins and banknotes) used by European citizens are the same, that is, they have the same value in the different countries, but not the euros that are deposited in the private banks of each Member State , which do not have the same value. For this reason, to guide the European Economic Area towards a true Monetary and Banking Union, the launch of a Digital Euro issued by the ECB would be a fundamental step[21].

4. CONCLUSION

The rise of the cryptocurrency sector has sparked a reaction from international banking and financial authorities. While cryptocurrencies have a decentralized structure and for the moment are only acting as a store of value in the face of the devaluation of fiat money, central bank projects present their CBDCs as a centralized electronic currency, a liquid and safe asset that would have a triple use: cash, deposit of value and means of payment.

The ECB is currently immersed in its own CBDC project. France and the Netherlands are leading progress among Member States. The first developments show a determined commitment by the European Union to the creation of a central bank digital currency that, if implemented, will revolutionize the world financial system. In this sense, the European Union has before it the opportunity to promote the Monetary and Banking Union, placing itself at the forefront of the financial digital revolution, in which the CBDC would be integrated into the new pan-European payment platform, based on crypto and programmable.

REFERENCES:

BCE, "Exploring anonymity in central bank digital currencies", 4 December 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Bindseil, U., "Tiered CBDC and the financial system", ECB Working Paper Series, Nº 2351, January 2020.

BIS, Impending arrival – a sequel to the survey on central bank digital currency, BIS Papers, Nº 107, 2020.https://www.bis.org/publ/bppdf/bispap107.pdf

Brunnermeier, M.K., Landeau, J.P. y James, H., "The Digitalization of Money", University of Princeton, August 2019. (https://scholar.princeton.edu/sites/default/files/markus/files/02c_digitalmoney.pdf).

Bundesverband deutscher Banken, "Following the debate on Facebook's "Libra" currency, German banks say: The economy needs a programmable digital euro!", 30 October 2019. https://bankenverband.de/media/files/Paper_programmable-digital-euro.pdf

DNP, "Central Bank Digital Currency: Objectives, preconditions and design choices", 2020. (https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2020/dnb388309.jsp

FinTechRat beim Bundesministerium der Finanzen, "Der digitale,programmierbare Euro", 2020. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Finanzmarktpolitik/2020-07-08-fintechrat-digitaler-euro.pdf?__blob=publicationFile&v=3

Mayer, Th., "A digital euro to save EMU", Vox EU-CEPR, 6 November 2019 (https://voxeu.org/article/digital-euro-save-emu).

Mersch, Y., "An ECB digital currency – a flight of fancy?", 11 March 2020 (https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html).

MIT, "Redesigning digital money: What can we learn from a decade of cryptocurrencies?", Digital Currency Initiative, MIT Media Lab, 22 January 2022.

Panneta, F., "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis", The ECB Blog, 28 Abril 2020. (https://www.ecb.europa.eu/press/blog/date/2020/html/ecb.blog200428~328d7ca065.en.html).

The Wall Street Journal, "Former Regulator Known as 'Crypto Dad' to Launch Digital-Dollar Think Tank", 16 January 2020.

The Wall Street Journal, "We Sent a Man to the Moon. We Can Send the Dollar to Cyberspace", 15 October 2019.

WEF, "Central Bank Digital Currency Policy-Maker Toolkit", White Paper, 22 January 2020. https://www.weforum.org/whitepapers/central-bank-digital-currency-policy-maker-toolkit

[21] Mayer, Th., "A digital euro to save EMU", Vox EU-CEPR, 6 November 2019 (https://voxeu.org/article/digital-euro-save-emu).

¿El futuro de la contratación?: Problemática jurídica del llamado legal smart contract

Álvaro Martín Sierra. ICADE

La contratación no es una realidad estática, sino que evoluciona junto con la realidad jurídica, económica y social del entorno en el que opera. En este contexto cambiante, los llamados smart contracts, o contratos inteligentes, se han convertido en una cuestión de gran interés en el ámbito de la práctica jurídica. No es para menos, ya que la irrupción de la tecnología de la cadena de bloques que los hace posibles puede suponer para la actividad legal una revolución y un cambio de paradigma absoluto en la forma de entender la contratación.

Si bien aún se encuentran lejos de la adopción masiva, los smart contracts se han adentrado ya en una fase de estandarización y desarrollo técnico que ha hecho posible la transformación de prácticas industriales y una nueva forma de concebir las interacciones con terceras partes. Esto resulta fundamental, pues solamente unos estándares internacionales pueden llegar a permitir la interoperabilidad entre los distintos tipos de contratos inteligentes y el desarrollo de un ecosistema sólido.

Un análisis de esta tecnología debe comenzar necesariamente por señalar las múltiples acep-

ciones de smart contract en la actualidad. La divergencia de posturas acerca de la naturaleza del contrato inteligente es tal que ha llegado a convertir el término "contrato" en equívoco. Esto se debe a que cuando se utiliza no se está haciendo referencia, salvo excepciones, a un acuerdo con plena fuerza legal. Es decir, por norma general, al hablar de contratación inteligente no debe asumirse que se está hablando de contratación en el sentido jurídico-privado de la expresión, sino de un concepto exclusivamente tecnológico.

Esta pluralidad de opiniones doctrinales ha llevado a que los esfuerzos iniciales de estandarización internacional persigan alcanzar un consenso acerca de la definición misma de smart contract.

En este sentido, la Unión Internacional de Telecomunicaciones (ITU), el organismo especializado de las Naciones Unidas en el ámbito de las telecomunicaciones y en las tecnologías de la información y la comunicación, se ha convertido en una de las principales referencias en la materia. Conviene destacar, entre sus múltiples iniciativas,

el documento técnico D 1.1 publicado en agosto de 2019 por el grupo de trabajo ITU-T. Dicho documento técnico, basado en iniciativas anteriores, como la planteada por el comité ISO/TC 307 en 2016, propone un marco de términos y definiciones en el ámbito de la tecnología de registro distribuido o DLT[1]. En concreto, se trata de uno de los primeros informes que proponen una definición de smart contract, como un "programa grabado en el sistema de registro distribuido que codifica las reglas para tipos específicos de transacciones[2] del sistema de registro distribuido de manera que pueda ser validado y activado por condiciones específicas".

Frente a esta definición genérica de smart contract, ITU-T propone en su documento técnico D 4.1 un marco regulatorio básico para la tecnología DLT a nivel mundial, introduciendo el concepto de "contrato inteligente para uso legal" o legal smart contract. Para ello, el grupo de trabajo plantea una serie de elementos que sustenten una posible definición de contrato inteligente a efectos legales en relación con las cuestiones regulatorias y de gobernanza que pudieran surgir en las primeras implementaciones de esta tecnología. Dichos elementos conforman lo que el documento técnico denomina "estructura de derecho contractual", y que supondría contar con un verdadero negocio jurídico encriptado en la red nodal.

Así, la lectura conjunta de las iniciativas de estandarización ITU-T DLT D 1.1 y D 4.1 ponen de manifiesto la necesidad de distinguir, para facilitar un espacio común de entendimiento, dos nociones de contrato inteligente: una tecnológica y otra legal.

---

[1] La cadena de bloques es solamente uno de los usos principales de la tecnología DLT. Debe precisarse que, si bien la tecnología de registro distribuido subyace a blokchain, no toda DLT es necesariamente una blockchain.

[2] Nótese que el término "transacción" no hace referencia a una operación de mercado o de naturaleza dineraria, sino a toda modificación o intercambio de información en esta tecnología de comunicación digital.

En tanto no se haga referencia al posible uso legal del smart contract, debe manejarse siempre una definición puramente tecnológica del citado contrato inteligente. Es decir, en el contexto de la cadena de bloques, un contrato inteligente no es más que un código que ejecuta en la cadena una función o funciones concretas cuando se cumple una condición previamente establecida. No se habla de "contrato" como de acuerdo legal vinculante en el sentido de la teoría general del contrato, sino de un software compuesto por instrucciones condicionales, siguiendo una estructura de ifs + thens, esto es, "si se da una situación A, entonces haz B".

Ahora bien, como se adelantaba al principio, la tecnología que hace posibles los contratos inteligentes puede también dar lugar a nuevas formas de acuerdos contractuales, desplazándonos a una primera fase de digitalización de la contratación. Al poder ser utilizados como mecanismos automatizados de cumplimiento contractual y, por tanto, como fuentes productoras de hechos jurídicos, los contratos inteligentes podrían añadir el adjetivo "legal".

Siempre que cumplan con los requisitos legales para predicar su naturaleza contractual —lo que sin duda exigirá su estudio caso por caso— podría hablarse del legal smart contract como de verdadero acuerdo entre partes, con plena eficacia obligacional, y no solamente como una máquina física de ejecución.

APROXIMACIÓN AL FENÓMENO DE LA CONTRATACIÓN INTELIGENTE EN LA PRÁCTICA JURÍDICA ESPAÑOLA

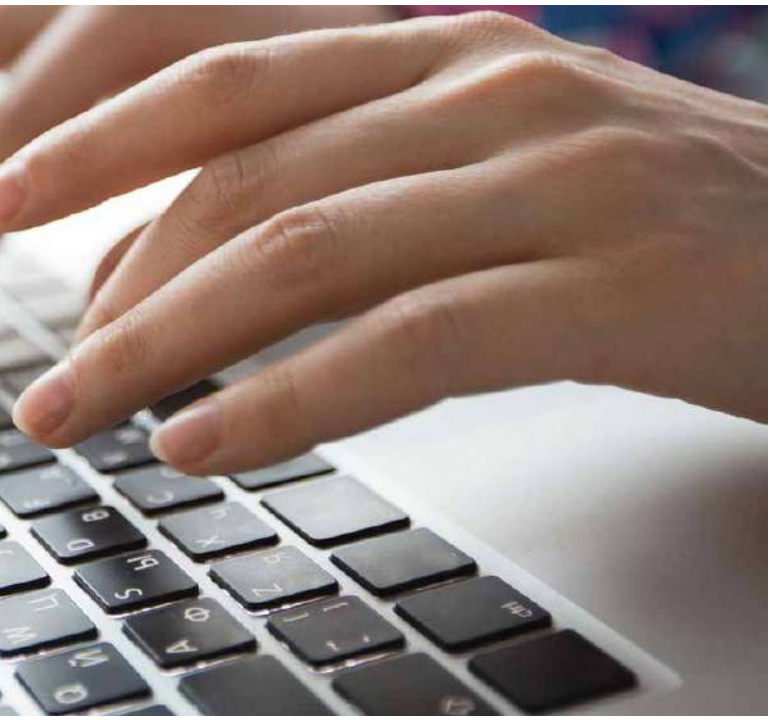
Podemos encontrar en la práctica jurídica española diversas aproximaciones al fenómeno de la contratación electrónica. Si bien estas han tenido su reflejo en la aprobación de normativa y regulación específica, como la Ley 34/2002, de 11 de julio, de servicios de la sociedad de información y de comercio electrónico, no existe aún consenso sobre si un contrato inteligente puede ser, por sí mismo, un contrato de Derecho privado. En este contexto, podemos distinguir dos posiciones doctrinales destacadas, como son la teoría de "code is law" y la "negadora".

Una de las posiciones doctrinales más relevantes en relación con la naturaleza de los contratos inteligentes es la llamada code is law

CODE IS LAW

Una de las posiciones doctrinales más relevantes en relación con la naturaleza de los contratos inteligentes es la llamada code is law o "el código (informático) es la ley".

Los defensores del code is law postulan que el espacio legal de creación de derechos que posibilita la contratación con terceros debe entenderse dividido en dos secciones distintas, la del espacio físico y la correspondiente al espacio virtual. Y estas dos secciones deben distinguirse de manera clara porque el funcionamiento y las normas que rigen la contratación en cada una de ellas es distinto. Por un lado, el espacio físico se ve gobernado por constituciones,



estatutos, códigos legales y por la redacción de los contratos tradicionales, no tecnológicos. Por otro lado, la regulación en el espacio virtual emana del propio código informático.

Según esta teoría, todos los dispositivos que permiten el acceso al espacio virtual existen para desempeñar unas funciones determinadas, que han sido incorporadas en su software por sus programadores. En la medida en que es este software el que determina la operativa y la eventual contratación en dicho espacio virtual, podría hablarse de una suerte de "Lex Informatica" o de un "Código del ciberespacio"[3].

Estos postulados chocan frontalmente con las iniciativas de estandarización comentadas en el apartado anterior. Incluso suponiendo que todo contrato inteligente tuviera un uso legal en un espacio de contratación virtual, sería necesario distinguir aquellos smart contracts actuando como mero medio de documentación de acuerdos de las verdaderas fuentes de obligaciones jurídicas[4]. Estos últimos son los únicos que podrían llegar a ser aceptados como forma de contratación según Derecho español.

Considero que la teoría del code is law acierta al plantear la necesidad de tratar de una forma jurídica distinta la operativa contractual en el mundo físico y el espacio virtual. Sin embargo, las características técnicas inherentes al software no son, por sí mismas, suficientes para predicar en todo caso su naturaleza contractual. Si bien nos encontramos ante una potencial forma de contratación que requiere de un tratamiento legal específico, esta tiene que basarse necesariamente en los principios básicos de la contratación ya utilizados en el mundo físico.

TEORÍA NEGADORA

La segunda de estas hipótesis doctrinales, llamada negadora, afirma que la estructura y desenvolvimiento técnico de los contratos inteligentes no tiene relevancia desde la óptica del Derecho de los contratos. Sin duda, esta posición dificulta el desarrollo de regulación de este fenómeno tecnológico aún más que la posible inseguridad jurídica derivada de una postura próxima al code is law.

Manejando un concepto puramente tecnológico del smart contract, esta teoría llega a la conclusión de que un contrato inteligente no es más que una máquina de ejecución, cuyas consecuencias legales dependerán de un contrato "tradicional", físico.

Este tipo de postulados también ignoran los estándares actuales, al prescindir en todo caso de un posible uso legal del contrato inteligente. Al manejar un concepto meramente técnico, los defensores de esta postura entienden que no cabe hablar de smart contracts como realidad jurídica.
Frente a esto cabe destacar que el Código Civil

[3] Tal y como lo definen autores como Joel Reidenberg y William Mitchell, respectivamente.

[4] La documentación del acuerdo cumpliría una función pasiva, con cabida en el marco actual de contratación electrónica. Sin embargo, el uso de un smart contract como contrato por sí mismo, sin soporte físico que lo acompañe, cumpliría una función activa, con difícil encaje en el ordenamiento actual, tal y como sostiene el Consejo General de la Abogacía Española en https://www.abogacia.es/publicaciones/blogs/blog-nuevas- tecnologias/contratos-inteligentes-los-smart-contract/. El software trascendería la definición pasiva de la Ley 34/2002 y dejaría de ser un mero instrumento de facilitación de consulta.

español sigue el sistema espiritualista, estableciendo su artículo 1278 que "los contratos serán obligatorios, cualesquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez". Es decir, dos partes interesadas podrían gozar de la libertad de forma en su contratación para adoptar una forma específica, la del lenguaje criptográfico del smart contract, para efectuar la manifestación digital de la prestación del consentimiento y consiguiente acuerdo de voluntades con unos efectos concretos.

En definitiva, si atendemos a los estándares desarrollados en esta materia, llegaremos a la conclusión de que es posible proponer y defender en la práctica española una posible noción legal de contrato inteligente.

La única postura aceptable desde la óptica de la estandarización será, por tanto, una postura intermedia, que supedite la naturaleza contractual de los smart contracts al cumplimiento de unos requisitos básicos.

Posibles dificultades en la aplicación práctica de un legal smart contract.

Supongamos que dos sujetos, X e Y, profesionales del sector petrolífero, deciden, ante la tangible implantación de distintas aplicaciones de blockchain en los contratos financieros de su actividad cotidiana, suscribir el día 21 de marzo de 2020 un contrato OTC de futuro sobre petróleo crudo West Texas Intermediate utilizando un contrato inteligente incorporado en la red Ethereum.

El contenido del contrato es el habitual en un contrato físico tradicional del sector: una parte, X, se compromete a comprar en el plazo de un mes una cantidad determinada de crudo, a un precio determinado, y la otra parte, Y, se compromete a venderlo[5]. Al tratarse de petróleo WTI, la liquidación del contrato se produce por entrega física de los barriles.

Sin embargo, este contrato presenta una gran particularidad. Al haberse elaborado íntegramente en lenguaje código como contrato inteligente e incorporado a la red Ethereum, sus datos son ahora inmutables e indelebles. Los scripts —archivos de instrucciones condicionales que se ejecutan de manera autónoma según su código— permanecerán seguros e intactos durante el tiempo que permanezca activo el libro registro de la red.

Los scripts permanecerán seguros e intactos durante el tiempo que permanezca activo el libro registro de la red.

El día 20 de abril del mismo año, un terremoto de magnitud 6,5 en la escala de Richter causa graves daños en la zona donde Y tenía almacenado el petróleo destinado a la entrega. El desplazamiento de la mercancía y, por tanto, el cumplimiento del contrato, deviene imposible. Así, esta circunstancia inevitable exige la modificación a posteriori del script del contrato inteligente, para poder seguir manteniendo la relación contractual adaptada a la nueva situación. Por este incidente difícilmente previsible, la inmutabilidad de la operativa en blockchain pasa de ser uno de sus principales atractivos a su mayor dificultad de implantación.

Ante una situación como la descrita, las opciones por parte de quien gobierna la red de intervenir el smart contract para modificar sus efectos ex post son muy reducidas.

Podría pensarse que, al tratarse de un contrato de ejecución automática, las partes no pueden llevar a cabo ninguna modificación de dicho contrato con posterioridad. Si bien técnicamente esto es así, podría incorporarse a la red

---

[5] Este tipo de instrumentos financieros resultan de gran utilidad para los productores de materias primas, se asegura el precio al que venderá sus existencias en el futuro, protegiéndose del riesgo de un cambio significativo de precios.

otro contrato inteligente con efectos prácticos exactamente contrarios a los del inicial: en lugar de "si se da A, haz B" podría programarse como "si se da A, haz C", siendo B y C opuestos.

Esta solución sería muy poco satisfactoria, pero es relevante precisar que este tipo de tecnologías ejecutables se centran en medidas de seguridad preventivas, ex ante, a expensas de las correctivas, ex post[6]. Si lo que se pretende es una modificación de los términos del legal smart contract, esta solamente será posible si el contrato se ha configurado para que pueda ser modificado bajo unas circunstancias concretas, de manera previa a la aceptación-ejecución del mismo.

Otra forma de prever futuras modificaciones sería configurar en el código informático una cláusula abierta de fuerza mayor. Una cláusula así posibilitaría la negociación posterior entre las partes y la delimitación del supuesto concreto, determinando un oráculo que insertase la información como transacción en la cadena de bloques. Al establecer la información externa del oráculo con posterioridad, podría modificarse la operativa del contrato inteligente.

Sin embargo, estas situaciones anormales no tienen por qué ser solucionadas exclusivamente en la cadena de bloques. En supuestos de incumplimiento contractual que requiera restitución, el ya citado informe técnico ITU-T DLT D 4.1 plantea que podría llegar a ser necesario acudir a formas de ejecución off-chain, esto es, en el mundo físico, fuera de la cadena. Si bien el código del smart contract tiene capacidad de ejecución de las transacciones sobre activos gestionados en una red DLT, otras condiciones del contrato requieren de medios de ejecución tradicionales[7].

La tecnología de la cadena de bloques permite cumplir automáticamente los términos de un acuerdo, aumentando de manera considerable la eficacia en la ejecución del mismo y reduciendo sus costes asociados, prescindiendo de intermediarios. Sin embargo, los legal smart contract no son una fórmula exenta de dificultades.

El nivel de madurez y desarrollo actual de esta nueva forma de contratación no permite hablar aún de implantación tangible, pero puede que la estandarización y los esfuerzos legislativos por regular este fenómeno nos permitan alcanzar un próspero futuro de contratación digital.

REFERENCIAS:

Giuffrida, I., Lederer, F. y Vermerys, N., A Legal Perspective on the Trials and tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law, Case Western Reserve Law Review, vol. 68 n. 3, 2018.

Ibáñez Jiménez, J. W., Derecho de Blockchain y de la tecnología de registros distribuidos, Aranzadi, Pamplona, 2018.

Ibáñez Jiménez, J. W., Blockchain: primeras cuestiones en el ordenamiento español, Dykinson, Madrid, 2018.

Savelyev, A. "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law", Higher School of Economics Research Paper No. WP BRP 71/LAW, 2016 (disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241).

Feliu Rey, J., "Smart Contract: concepto, ecosistema y principales cuestiones de Derecho privado", La Ley Mercantil, nº 47, 2018.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. y Goldfeder, S., "Bitcoin and Cryptocurrency Technologies", Princeton University, 2016 (disponible en https://www.lopp.net/pdf/princeton_bitcoin_book.pdf).

ITU-T, Technical Specification FG DLT D1.1. Distributed ledger technology terms and definitions. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), 2019.

ITU-T, Technical Report FG DLT D4.1. Distributed ledger technology regulatory framework. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), 2019.

[6] Narayanan, A., Bonneau, J., Felten, E., Miller, A. y Goldfeder, S., "Bitcoin and Cryptocurrency Technologies", Princeton University, 2016.

[7] Ibáñez Jiménez, J. W., Derecho de Blockchain y de la tecnología de registros distribuidos, Aranzadi, Pamplona, 2018, p. 56 y ss.

The future of contracting? Legal issues of the so-called legal smart contract

Álvaro Martín Sierra. ICADE

Contracting is not a static reality, but evolves along with the legal, economic and social reality of the environment in which it operates. In this changing context, the so-called smart contracts have become a matter of great interest in the field of legal practice. This is not to be underestimated, since the irruption of blockchain technology that makes them possible may represent for legal activity a revolution and an absolute change of paradigm in the way of understanding contracting.

Although still far from being massively adopted, smart contracts have already entered a phase of standardization and technical development that has made possible the transformation of industrial practices and a new way of conceiving interactions with third parties. This is essential, as only international standards can enable interoperability between different types of smart contracts and the development of a robust ecosystem.

An analysis of this technology must necessarily begin by pointing out the multiple meanings of

smart contract today. The divergence of positions on the nature of the smart contract is such that it has come to make the term "contract" misleading. This is because when it is used it is not referring, with exceptions, to an agreement with full legal force. In other words, as a general rule, when talking about intelligent contracting it should not be assumed that we are talking about contracting in the private-law sense of the expression, but rather of a purely technological concept.

This wide range of doctrinal views has led to initial international standardization efforts to reach a consensus on the very definition of a smart contract.

In this regard, the International Telecommunication Union (ITU), the United Nations' specialized agency in the field of telecommunications and information and communication technologies, has become one of the main references in this field. Among its many initiatives, technical document D 1.1 published in August 2019 by the ITU-T working group should be highlighted. This technical document, based on previous initiatives, such as that proposed by the ISO/TC 307 committee in 2016, proposes a framework of terms and definitions in the field of distributed ledger technology or DLT[1]. In particular, it is one of the first reports to propose a definition of a smart contract as a "program recorded in the distributed ledger system that encodes the rules for specific types of transactions[2] in the distributed ledger system so that it can be validated and activated under specific conditions".

As opposed to this generic definition of smart contract, ITU-T proposes in its technical document D 4.1 a basic regulatory framework for DLT technology at a world-wide level, introducing the concept of "smart contract for legal use" or legal smart contract. To this end, the working group proposes a series of elements to support a possible definition of a smart contract for legal purposes in relation to the regulatory and governance issues that could arise in the first implementations of this technology. These elements conform what the technical document calls a "contract law structure", which would mean having a real legal transaction encrypted into the nodal network.

Thus, a read together of the ITU-T DLT D 1.1 and D 4.1 standardization initiatives shows the need to distinguish, in order to facilitate a common space of understanding, two notions of smart contract: the technological one and the legal one.

As long as no reference is made to the possible legal use of the smart contract, a purely technological definition of the smart contract must always be handled. That is to say, in the context of the blockchain, a smart contract is nothing more than code that executes a specific func-

[1] Blockchain is only one of the main uses of DLT technology. It should be noted that while distributed ledger technology underlies blokchain, not all DLT is necessarily a blockchain.

[2] Please note that the term "transaction" does not refer to an operation of a market or monetary nature, but to any modification or exchange of information using this digital communication technology.

tion or functions in the chain when a previously established condition is met. We do not speak of a "contract" as a legally binding agreement in the sense of the general theory of contract, but of a software consisting of conditional instructions, following a structure of ifs + thens, i.e. "if a situation A occurs, then do B".

However, as anticipated at the outset, the technology that makes smart contracts possible can also lead to new forms of contractual arrangements, moving us into a first phase of contract digitization. As they can be used as automated mechanisms of contractual compliance and, therefore, as agreements producing legal effects, smart contracts could add the adjective "legal". Provided that they meet the legal requirements to preach their contractual nature —which will undoubtedly require their study on a case-by-case basis— we could speak of the legal smart contract as a true agreement between parties, with full binding effect, and not just as a physical execution machine.

AN APPROACH TO THE PHENOMENON OF SMART CONTRACTING IN SPANISH LEGAL PRACTICE

In Spanish legal practice, we can find various approaches to the phenomenon of electronic contracting. Although these have been reflected in the approval of specific rules and regulations, such as Law 34/2002, of July 11th, on information society services and electronic commerce, there is still no consensus on whether a smart contract can be, in itself, a private law contract. In this context, we can distinguish two major doctrinal positions, namely the "code is law" theory and the "denialist" theory.

CODE IS LAW

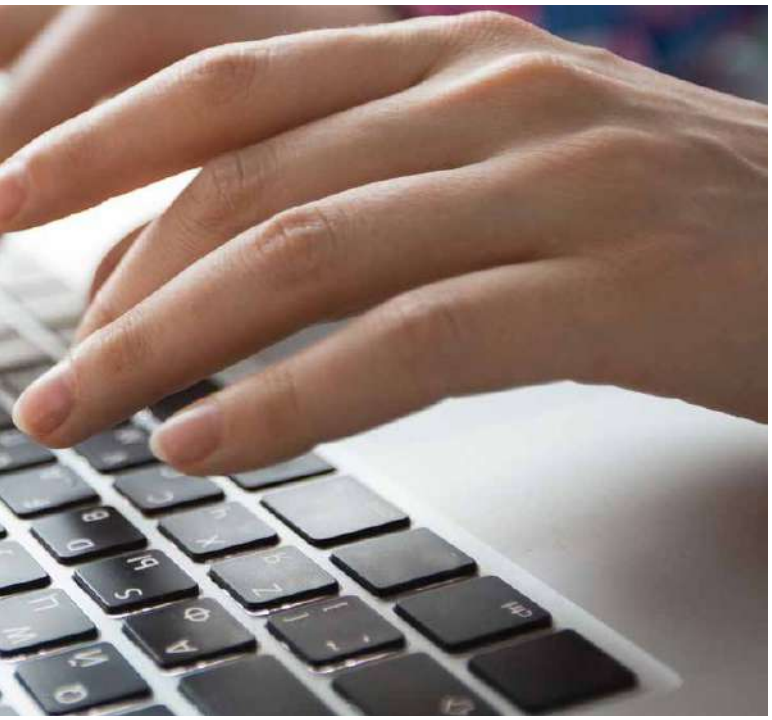
One of the most relevant doctrinal positions regarding the nature of smart contracts is the so-called (computer) code is law.

The advocates of Code is Law postulate that the legal space for creating rights that makes contracting with third parties possible should be understood to be divided into two distinct

One of the most relevant doctrinal positions regarding the nature of smart contracts is the so-called (computer) code is law

sections, that of physical space and that of virtual space. These two sections must be clearly distinguished because the operation and rules governing contracting in each of them are different. On the one hand, the physical space is governed by constitutions, statutes, legal codes and the drafting of traditional, non-technological contracts. On the other hand, regulation in virtual space stems from the computer code itself.

According to this theory, all devices that allow access to virtual space exist to perform certain functions, which have been incorporated into their software by their programmers. To the extent that it is this software that determines the operation and eventual contracting in this virtual



space, one could speak of a sort of "Lex Informatica" or a "Cyberspace Code"[3].

These postulates clash head-on with the standardization initiatives discussed in the previous section. Even assuming that every smart contract has a legal use in a virtual contracting space, it would be necessary to distinguish those smart contracts acting as mere means of documentation of agreements from the real sources of legal obligations[4]. The latter are the only ones that could be accepted as a form of contracting under Spanish law.

I believe that the theory of the code is law is right in raising the need to treat contractual operations in the physical world and virtual space in a different legal form. However, the technical characteristics that are inherent in software are not, in themselves, sufficient to preach its contractual nature in every case. Although this is a potential form of contracting that requires specific legal treatment, it must necessarily be based on the basic principles of contracting already used in the physical world.

DENIALIST THEORY

The second of these doctrinal positions, called "denialist", states that the structure and technical development of smart contracts has no relevance from the perspective of contract law. This position undoubtedly makes the development of regulation of this technological phenomenon even more difficult than the possible legal uncertainty resulting from a pro code is law approach.

Using a purely technological concept of the smart contract, this theory concludes that a smart contract is nothing more than an execution machine, the legal consequences of which will depend on a "traditional", physical contract.

This type of postulate ignores the current standards as well, by dispensing in any case with a possible legal use of the intelligent contract. By using a purely technical concept, the advocates of this position understand that smart contracts cannot be spoken of as a legal reality.

Opposite to this, it should be noted that the Spanish Civil Code follows the spiritualist system, establishing in its article 1278 that "contracts shall be obligatory, whatever form they have taken, provided that they contain the essential conditions for their validity". That is to say, two interested parties could enjoy freedom of form in their contracting to adopt a specific form, that of the cryptographic language of the smart contract, to effect the digital manifestation of the provision of consent and consequent agreement of wills with specific effects.

In definitive, if we attend to the standards developed in this matter, we will reach the conclusion that

---

[3] As defined by authors such as Joel Reidenberg and William Mitchell, respectively.

[4] The documentation of the agreement would play a passive role, which would fit into the current legal framework of electronic contracting. However, the use of a smart contract as a contract in itself, without any physical support to accompany it, would fulfill an active function, which would be difficult to fit into the current system, as the General Council of Spanish Lawyers maintains at https://www.abogacia.es/publicaciones/blogs/blog-nuevas-tecnologias/contratos-inteligentes-los-smart- contract/. The software would transcend the passive definition of Law 34/2002 and would no longer be a mere instrument for facilitating consultation.

it is possible to propose and defend in the Spanish practice a possible legal notion of smart contract.

The only acceptable position from the point of view of standardization will therefore be an intermediate one, which makes the contractual nature of smart contracts dependent on the fulfillment of basic requirements.

POSSIBLE DIFFICULTIES ENCOUNTERED IN THE PRACTICAL APPLICATION OF A LEGAL SMART CONTRACT

Let us suppose that two subjects, X and Y, professionals in the oil sector, decide, in view of the tangible implementation of different blockchain applications in the financial contracts of their daily activity, to enter into a West Texas Intermediate OTC crude oil futures contract on March 21st, 2020 using a smart contract built into the Ethereum network.

The content of the contract is the usual one in a traditional physical contract in the sector: one party, X, undertakes to buy within one month a certain quantity of crude oil, at a certain price, and the other party, Y, undertakes to sell it[5]. As the oil is WTI, the contract is settled by physical delivery of the barrels.

However, this contract has one major peculiarity. Having been drafted entirely in code language as a smart contract and incorporated into the Ethereum network, its data are now immutable and indelible. The scripts —conditional instruction files that are executed autonomously according to their code— will remain safe and intact as long as the network ledger remains active.

On April 20th of the same year, an earthquake of magnitude 6.5 on the Richter scale causes serious damage in the area where Y had stored the oil for delivery. The movement of the goods and therefore the fulfillment of the contract becomes impossible.

This unavoidable circumstance thus requires the subsequent modification of the smart contract script, in order to continue maintaining the contractual relationship adapted to the new situation. Due to this incident, which is difficult to predict, the immutability of the blockchain operation has gone from being one of its main attractions to its greatest difficulty in implementation.

The scripts will remain safe and intact as long as the network ledger remains active.

In a situation like the one described, the options for those who govern the network to intervene in the smart contract to modify its effects ex post are very limited.

It might be thought that, as this is an automatically enforceable contract, the parties cannot make any amendments to the contract at a later date. Although technically this is the case, another smart contract could be incorporated into the network with practical effects exactly opposite to those of the initial one: instead of "if A is given, beam B" it could be programmed as "if A is given, beam C", with B and C being opposite.

This solution would be very unsatisfactory, but it is important to specify that this type of executable technology focuses on preventive, ex-ante,

[5] This type of financial instrument is very useful for commodity producers, as it secures the price at which they will sell their stocks in the future, protecting them from the risk of significant price changes.

at the expense of corrective, ex- post security measures[6]. If the intention is to modify the terms of the legal smart contract, this will only be possible if the contract has been configured so that it can be modified under specific circumstances, prior to the acceptance-execution of the contract.

Another way of providing for future modifications would be to configure an open clause of force majeure in the computer code. Such a clause would make it possible to negotiate later between the parties and to delimit the specific case, determining an oracle that would insert the information as a transaction in the blockchain. By establishing the external information of the oracle later, the operation of the smart contract could be modified.

However, these abnormal situations do not have to be solved exclusively in the blockchain. In cases of breach of contract requiring restitution, the aforementioned ITU- T DLT D 4.1 technical report suggests that it may be necessary to resort to off-chain forms of enforcement, i.e. in the physical world, outside the chain. Although the smart contract code has the capacity to execute transactions on assets managed in a DLT network, other contract conditions require traditional means of execution[7].

The blockchain technology allows the terms of an agreement to be met automatically, considerably increasing efficiency in the execution of the agreement and reducing its associated costs, by dispensing with intermediaries. However, legal smart contracts are not a formula without difficulties.

The current level of maturity and development of this new form of contracting does not yet allow us to speak of tangible implementation, but it may be that standardization and legislative efforts to regulate this phenomenon will allow us to achieve a prosperous future of digital contracting.

REFERENCIAS:

Giuffrida, I., Lederer, F. y Vermerys, N., A Legal Perspective on the Trials and tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law, Case Western Reserve Law Review, vol. 68 n. 3, 2018.

Ibáñez Jiménez, J. W., Derecho de Blockchain y de la tecnología de registros distribuidos, Aranzadi, Pamplona, 2018.

Ibáñez Jiménez, J. W., Blockchain: primeras cuestiones en el ordenamiento español, Dykinson, Madrid, 2018.

Savelyev, A. "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law", Higher School of Economics Research Paper No. WP BRP 71/LAW, 2016 (disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241).

Feliu Rey, J., "Smart Contract: concepto, ecosistema y principales cuestiones de Derecho privado", La Ley Mercantil, nº 47, 2018.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. y Goldfeder, S., "Bitcoin and Cryptocurrency Technologies", Princeton University, 2016 (disponible en https://www.lopp.net/pdf/princeton_bitcoin_book.pdf).

ITU-T, Technical Specification FG DLT D1.1. Distributed ledger technology terms and definitions. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), 2019.

ITU-T, Technical Report FG DLT D4.1. Distributed ledger technology regulatory framework. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), 2019.

[6] Narayanan, A., Bonneau, J., Felten, E., Miller, A. y Goldfeder, S., "Bitcoin and Cryptocurrency Technologies", Princeton University, 2016.

[7] Ibáñez Jiménez, J. W., Derecho de Blockchain y de la tecnología de registros distribuidos, Aranzadi, Pamplona, 2018, p. 56 y ss.

Gestão e governança de **mudanças para aplicações** descentralizadas

Suzana Maranhao.
Digital Innovation Analyst (DLT/Blockchain)

MOTIVAÇÃO

O desenvolvimento de aplicações utilizando a tecnologia blockchain[1] viabiliza a criação de novos modelos de negócio em diversos setores da economia com potencial para endereçar em larga escala desafios importantes na nossa sociedade, por ser capaz de aumentar a confiança nas relações entre as partes.

Desde que não existam ataques bem-sucedidos ou conluio entre nós, uma rede blockchain, descentralizada e sincronizada por um algoritmo de consenso, viabiliza um ambiente de execução de software imutável. Às partes envolvidas é garantido que a execução do código on-chain sempre corresponderá ao especificado no código do contrato inteligente. Conforme discutido no artigo de Kevin Werbach (Werbach, 2018), a imutabilidade é chave para a criação de confiança entre partes sem necessidade de envolver autoridades centralizadas, mas também potencializa falhas nas relações no curto, médio ou longo prazo, muitas vezes sem fácil mecanismo para resolução de conflitos.

A tecnologia não pode garantir que o código do contrato inteligente realmente reflita o que

[1] *Este texto usa o termo blockchain e DLT como sinônimos, por simplicidade.*

deveria ser executado. Por exemplo, pode ter existido um erro na especificação do código, fazendo com que sua execução não reflita os requisitos que o deram origem, como o famoso caso do The DAO. Também é possível que ocorra uma mudança no acordo entre as partes decorrente, por exemplo, de uma mudança de legislação, e que não seja possível adaptar o funcionamento do contrato inteligente para a nova realidade.

Considerando os benefícios de blockchain e a necessidade prática de atualização dos contratos inteligentes, a questão que este texto discute é como conciliar mudanças em aplicações que usam contratos inteligentes minimizando a perda de confiança das partes interessadas? Este texto descreve uma proposta de resposta a essa questão, que envolve a especificação de uma solução técnica integrada ao funcionamento de uma estrutura de governança.

Exemplo

Suponha o cenário de um contrato de financiamento que usa uma taxa fixa para cobrar um valor de quem solicitou o empréstimo e o destina a quem emprestou. É possível prever na codificação do contrato que o valor da taxa fixa pode mudar, que a mudança só pode ser realizada por um papel específico e que esse papel pode ser exercido por um conjunto de pessoas ao mesmo tempo. No entanto, caso algum requisito de negócio ou mesmo uma nova regulação implique que seja necessário alterar a cobrança para uma taxa variável, é possível que o código do contrato inteligente não seja flexível o suficiente para essa mudança. Como viabilizar a mudança da aplicação nesse cenário?

GOVERNANÇA DA APLICAÇÃO

Muito se discute sobre a governança de redes blockchain (Jimenéz, 2020) (Lyons and Courcelas, 2020). Sendo descentralizada, o gestor de cada nó de uma rede pode decidir autonomamente sobre questões operacionais e de evolução. Exemplos de questões envolvendo a governança da rede podem ser a entrada e a saída de nós na rede, mudanças de configuração do protocolo de consenso e evolução de versão de software a ser executado em um nó.

As aplicações que executam em redes blockchain, materializada em contratos inteligentes, também suscitam questões específicas a serem decididas pelas partes que possuam autoridade para tal, que serão chamadas de governança da aplicação. A governança de aplicação é a responsável por verificar que o código do contrato inteligente realmente faz o que deveria ser feito.

A ação de implantar um ou mais contratos inteligentes deve ser decorrente de uma decisão da governança da aplicação. Qualquer proposta de mudança em um contrato inteligente é também uma mudança na decisão original da governança da aplicação e deve, portanto, ser uma nova decisão do mesmo grupo.

Uma vez que as aplicações dependem da rede para executar, a correta execução dos contratos inteligentes também depende da governança da rede. Em alguns casos, especialmente em redes permissionadas que foram criadas para suportar um propósito específico, os membros da governança da rede podem ser os mesmos membros da governança da aplicação, mas essa coincidência de membros é um caso particular que não se repete sempre.

A governança de aplicação é a responsável por verificar que o código do contrato inteligente realmente faz o que deveria ser feito

As ações e as decisões da governança da aplicação muitas vezes acontecem de forma off-chain. As partes que possuem autoridade acordam o escopo que deve ser construído e muitas vezes contratam um executor para a implementação e a implantação. Na prática, essa delegação é uma relação de confiança da governança da aplicação para o executor.

Em uma maturidade mais alta, a governança da aplicação pode passar a ser suportada por um processo automatizado na própria blockchain, que permita minimizar a confiança no executor da mudança e compartilhar a responsabilidade pelas decisões. Esse processo será descrito mais adiante neste texto.

Níveis de confiança

Entre uma aplicação centralizada - que pode ser modificada a qualquer momento pelo seu gestor - e uma aplicação descentralizada imutável existe uma gradação de níveis de confiança. A confiança nos membros da governança da aplicação e no processo de mudança no qual a aplicação está inserida são determinantes para o nível de confiança que uma parte interessada tem na execução previsível da aplicação.

E A CONFIANÇA DE QUEM NÃO FAZ PARTE DA ESTRUTURA DE GOVERNANÇA?

Além da governança da aplicação, existem outros impactados com mudanças em contratos inteligentes. Sejam os usuários da aplicação ou observadores externos, essas pessoas, aqui chamadas de partes interessadas, confiam que o contrato inteligente faz o que deveria fazer. Os membros da estrutura de governança também são partes interessadas.

Partindo da premissa que um código especificado é imutável, as partes interessadas confiam na conformidade do contrato inteligente se elas leram e entenderam o código ou se confiam que a governança da aplicação (ou outras partes interessadas) verificou que o contrato inteligente realmente foi implementado com o comportamento esperado.

Considerando o esforço necessário para ler e entender o código, assume-se aqui que muitas partes interessadas simplesmente confiam na governança da aplicação. Importante destacar que órgãos de auditoria ou instituições credenciadas podem ser incluídos na governança da aplicação de forma a aumentar sua credibilidade.

Para aquelas partes interessadas que não confiam na governança da aplicação e desejam analisar o código imutável de forma independente, é necessário garantir que exista um mecanismo confiável que permita acompanhar o trabalho da governança e as mudanças a serem executadas.

É necessário garantir que exista um mecanismo confiável que permita acompanhar o trabalho da governança e as mudanças a serem executadas

O mencionado processo de mudança automatizado na própria blockchain, que permite maximizar a confiança entre os membros da governança, pode assim também maximizar a confiança das partes interessadas.

PROCESSO DE MUDANÇA E LEGALIDADE DA REDE

Um processo de mudança de aplicações descentralizadas é ainda mais relevante de ser implementada para o caso de redes que se propõem a manter a legalidade. Leis ou regulamentações podem ser modificadas e tornar contratos inteligentes ilegais se os códigos imutáveis não são flexíveis o suficiente para ser adequado a uma mudança que precise ser realizada. Um exemplo é um contrato inteligente que calcula o total de impostos a serem pagos. O que acontece se a regra de cálculo do valor for alterada? Além disso, ordens judiciais podem demandar uma alteração de dados ou mesmo do código de um contrato inteligente.

Por exemplo, uma ordem judicial pode alterar o valor de um parâmetro de cálculo de uma pensão a ser paga periodicamente ou sua fórmula de cálculo.

A ausência de mecanismo para evolução da aplicação faz com que seja necessário criar uma solução para efetivamente deixar a aplicação juridicamente legal. Uma solução é pausar a execução de contratos inteligentes e implantar novos contratos alterados envolvendo

A ausência de mecanismo para evolução da aplicação faz com que seja necessário criar uma solução para efetivamente deixar a aplicação juridicamente legal

os responsáveis por definir e aprovar as novas regras. Essa ação pode acarretar: (a) problemas de migração de dados com possível perda de informação, (b) impacto em aplicações externas que dependiam da aplicação modificada e (c) quebra de confiança das partes interessadas.

Uma solução mais elaborada e robusta é ter preparada a aplicação para executar vinculada a um processo de mudança. Dentro da mudança, assim como na solução anterior, novos contratos inteligentes também serão implantados, mas isso ocorrerá dentro de um processo conhecido e rastreável, que objetiva maximizar a confiança das partes interessadas e minimizar o impacto operacional.

REQUISITOS DO PROCESSO DE MUDANÇA PROPOSTO

Três requisitos em alto nível para um processo de mudança de aplicação são propostos a seguir. Todos devem ser atendidos por implementação on-chain, de forma a garantir a previsibilidade e confiança do processo.

1. Facilitar a evolução de uma aplicação que usa contratos inteligentes;
2. Garantir a transparência do processo de gestão de mudança para as partes interessadas;
3. Garantir que a governança da aplicação concorde com a conformidade da aplicação a ser implantada ou evoluída.

A evolução de aplicação citada no primeiro requisito pode abranger correção de defeitos de código, atualização de algum requisito de negócio ou alteração do estado de variáveis de contratos. São exemplos de facilidades que uma implementação capaz de atender ao primeiro requisito pode oferecer no contexto de uma mudança da aplicação: (a) preservar o acesso aos dados utilizados pela aplicação, minimizando migração de dados; (b) viabilizar uma forma de alteração de dados não prevista pelas regras de negócios da aplicação; (c) viabilizar uma forma de alteração de estrutura de dados, preservando o acesso aos dados utilizados pela aplicação; (d) expor uma forma imutável de encontrar a implementação atual dos contratos inteligentes; e (e) preservar a qualidade do código de contratos inteligentes ao longo do tempo, mesmo após várias evoluções.

Pelas características de uma rede blockchain, dados armazenados em transações para a rede não são alterados. Apenas é possível alterar o estado atual de dados armazenados em variáveis dos contratos inteligentes. Sendo assim, uma implementação do requisito 1 não é capaz de resolver a questão do direito ao esquecimento de leis de privacidade.

O segundo requisito garante a transparência no processo de gestão de mudança. Além de atender ao primeiro requisito, uma implementação que atende ao segundo requisito deve: (a) estabelecer que as mudanças seguem um ciclo de vida, que envolve especificação, aprovação, execução e conclusão, ou cancelamento; (b) relacionar a mudança com informações off-chain que detalham por exemplo a sua motivação e o desenho técnico que embasa a solução adota-

da; (c) viabilizar uma forma de especificar objetivamente, e preferencialmente de forma imutável, o script da mudança - de forma a permitir a análise desse script antes mesmo da aprovação da mudança; (d) prevenir a execução de mudanças que não são submetidas ao processo de mudança; (e) prover transparência de quais foram as mudanças propostas e o que aconteceu com essas propostas e (f) viabilizar um mecanismo para monitoração das mudanças em andamento.

Idealmente, a proposta de mudança começa a ser discutida de forma off-chain, de forma a facilitar o debate e a avaliação de impactos. Apenas quando os membros concordam com o que deve ser proposto é que uma mudança deve ser proposta utilizando o processo. De forma a relacionar a mudança com as informações off-chain (descrito no item 'b'), é possível, por exemplo, registrar na blockchain o hash do documento que registra a motivação, a discussão e a avaliação de impacto da mudança e, possivelmente, o desenho técnico que embasa a solução adotada. Uma forma de viabilizar a monitoração das mudanças (descrito no item 'f') pode ser emitir um evento para cada modificação de estado da mudança.

Uma forma de viabilizar a monitoração das mudanças pode ser emitir um evento para cada modificação de estado da mudança

O último requisito objetiva garantir que as partes que compõem a governança da aplicação concordem com a conformidade do contrato inteligente. Uma implementação que atende aos três requisitos citados deve então ter automatizado o conceito da estrutura de governança, capaz de decidir sobre mudanças com o objetivo de compartilhar a responsabilidade da mudança. Um mecanismo de votação pode apoiar o processo de tomada de decisão do grupo e os participantes podem ser identificados para que sua responsabilidade se reflita também no mundo real. Implementações podem optar por classificar mudanças em diferentes dificuldades de implantação, dependendo da avaliação do impacto da mudança. Deve ser também definida uma regra para a inclusão ou exclusão de membros na governança da aplicação e pode ser selecionado um subconjunto desses membros para votar cada mudança.

Conforme discutido anteriormente, as partes interessadas precisam confiar nas decisões do grupo de governança da aplicação. Um ponto importante a ser reforçado é que a estrutura de governança deve ser envolvida desde a primeira implantação dos contratos inteligentes da aplicação de forma a promover o compartilhamento da responsabilidade pela primeira implantação.

CONSIDERAÇÕES SOBRE USO DO PROCESSO DE MUDANÇA

Uma boa prática defendida em governança de redes públicas é o princípio da liberdade para sair da rede a qualquer momento, caso deseje ("you are free to opt out") (Lyons and Courcelas, 2020). A mesma prática pode ser aplicada à evolução de aplicações. O processo de mudança descrito não incluiu esse requisito obrigatório porque o tratamento dessa prática não é facilmente generalizável para ser tratada fora do código da aplicação. No entanto, é recomendado que a governança da aplicação avalie e se possível suporte essa prática na especificação de cada mudança.

O processo de mudança também não contempla a possibilidade de existir um delta de tempo entre a aprovação e a execução da mudança, o que daria às partes interessadas um tempo para decidir o que fazer considerando a mudança iminente da aplicação como também um tempo para a implementação de um mecanismo adicional de segurança. Essa possibilidade precisa ser discutida em mais detalhes.

Uma análise interessante de uma aplicação pode ser realizada ao observar o número e criticidade das mudanças submetidas, aprovadas e executadas. Muitas mudanças podem significar modificações constantes de requisitos de negócios ou descoberta de defeitos. Pela análise das informações geradas pelo processo de mudança, qualquer parte interessada pode entender o histórico e a previsão de mudanças da aplicação.

ANALOGIA COM BOAS PRÁTICAS DE TI

A proposta de estabelecer um processo para rastrear e formalmente decidir sobre mudanças não é nova dentro da gestão de serviços de TI. As boas práticas do ITIL(Axelos, 2019) contemplam a existência de um processo de gestão de mudança para garantir que as mudanças passem por um fluxo de atividades pré-definido, incluindo avaliação e aprovação. O objetivo é catalogar e distribuir as medidas que devem ser tomadas ao realizar mudanças e, se for o caso, minimizar o impacto de eventuais incidentes.

Dentro da realidade de aplicações em redes blockchain, o processo de mudança também é útil para assegurar que as mudanças possam ocorrer minimizando o impacto na confiança entre aqueles que compõem a governança da aplicação e as partes interessadas.

Exemplo de implementação do processo de mudança proposto

A plataforma Ethereum não oferece nativamente suporte aos requisitos descritos nesse texto, embora existam algumas implementações parciais da solução, como a do OpenZeppelin (OpenZeppelin, 2020), ERC1504 (Wu et al., 2017) e ERC930 (Lemble, 2018). Uma proposta de implementação que reaproveita parcialmente as implementações citadas pode ser encontrada em: https://github.com/bndes/BlockchainChangeManagementFramework.

Uma implementação de uma aplicação utilizando esse framework de gestão de mudança contém: (a) um conjunto de contratos inteligentes genéricos para o próprio processo de mudança, (b) contratos inteligentes criados especificamente para cada mudança e (c) os próprios contratos inteligentes da implementação da aplicação que pode ser atualizada.

REFERÊNCIAS:

Axelos (2019), ITIL® Foundation, ITIL 4 edition. Disponível em: https://openzeppelin.com/.

Jimenéz, J. W. I (2020), Alastria Mission and Vision, A Multidisciplinary Research, Reus Editorial.

Lemble, A. (2018), ERC930 - Eternal Storage Standard, Ethereum Improvement Proposals. Disponível em: https://github.com/ethereum/EIPs/issues/930

Lyons, T., Courcelas, L. (2020), Governance of and with Blockchains, EU Blockchain Observatory and Forum, Disponível em: https://www.eublockchainforum.eu/reports.

Axelos (2019), ITIL® Foundation, ITIL 4 edition. Disponível em: https://openzeppelin.com/.

OpenZeppelin (2020), Upgrading Smart Contracts, OpenZeppelin docs. Disponível em: https://docs.openzeppelin.com/learn/upgrading-smart-contracts.

Werbach, K. (2018), The Siren Song: Algorithmic Governance By Blockchain, in After the Digital Tornado: Networks, Algorithms, Humanity. Disponível em SSRN: https://ssrn.com/abstract=3578610.

Wu, K., Ren, C., He R., Ma, Y., Liu, X. (2017), ERC-1504 Upgradable Smart Contract, Ethereum Improvement Proposals. Disponível em: https://eips.ethereum.org/EIPS/eip-1504

Este é um projeto ainda em andamento. Por favor, entre em contato se quiser contribuir para o desenvolvimento deste trabalho.

Change management and governance for **decentralized applications**

Suzana Maranhao.
Digital Innovation Analyst (DLT/Blockchain)

MOTIVATION

The development of applications using the blockchain[1] technology enables the creation of new business models in various sectors of the economy and it has the potential to tackle, on a large scale, important challenges for our society, due to its ability to increase trust in the relationship among stakeholders. Provided that there are no successful attacks or collusion between nodes, a blockchain network, decentralized and synchronized by a consensus algorithm, will grant an immutable software execution environment. It is guaranteed to the stakeholders that the execution of the on-chain code will always correspond to what was specified in the smart contract code. As Kevin Werbach (Werbach, 2018) discusses it in his article, immutability is key to build trust among stakeholders, which rules out the need to involve centralized authorities, yet it does also increase failure risk in relations within a short, medium or long-term period and very often leaves no conditions for easy conflict troubleshooting.

Technology cannot make sure that the code of the smart contract will really reflect what

[1] *In this text, blockchain and DLT are used as synonymous.*

should be executed. For instance, there can exist an error in code specification, which may lead its execution to mismatch the requirements that originated it, like the known DAO case. A change in the agreement of the stakeholders can also occur, due to a change in legislation, for instance, which may render it impossible to adapt the smart contract to the new reality.

Bearing in mind the benefits of blockchain and the practical need to update the smart contracts, what this text is trying to approach is how to tackle changes in applications using smart contracts, in order to minimize the loss of trust among stakeholders? This text proposes an answer to this question, which involves the specification of a technical solution in combination with a governance structure.

Consider this example:

Let us consider the following scenario: a financing contract that uses a fixed tax to charge the borrower and that is intended for the lender. It is possible to establish in the contract coding that the fixed tax can vary, that this variation can be executed by a specific role player and that this role should be played by a set of people simultaneously. However, if some business requirement or some new regulation demands the change for a variable tax, the smart contract code may not be flexible enough for this change. How can one make the application change possible in this case?

APPLICATION GOVERNANCE

There is a lot of debate on the governance of the blockchain networks (Jimenéz, 2020) (Lyons and Courcelas, 2020). Considering they are decentralized, the manage, for of each node of a network can autonomously decide on operation and evolution issues. Some examples of issues that involve network governance are the entrance or the exit of nodes in a network, changes in the configuration of the consensus protocol and the evolution of a software version to be used in a node.

The blockchain applications, which can be materialized in smart contracts, also bring about specific issues to be decided upon by the stakeholders that have authority for that, which will be called hereafter application governance. Application governance is what ensures that the smart contract code does exactly what it should. The act of deploying one or more smart contracts is associated with an application governance decision. Any change in a smart contract is also a change in the original decision of the application decision and must therefore represent a new decision of the same group.

Since the applications depend on the network to execute, the correct execution of the smart contracts also depends on the network governance. In some cases, especially when the permissioned networks are created to serve a specific purpose, the network's governance members can be the same members of the application governance, but this is merely a coincidence and does not necessarily occur all the time.

Application governance is what ensures that the smart contract code does exactly what it should

Actions and decisions of the governance quite often occur off-chain. The stakeholders that possess authority agree on a scope that must be built and they quite often hire an executor for the development and the deployment. In practical terms, this delegation is rooted in the application governance's trust towards the executor.

Considering a more mature setting, application governance can occur through an automatized process in the blockchain network itself, one that allows minimizing trust in the change executor and sharing decision-making responsibilities. This text will describe this process later on.

Trust levels

One can come from a centralized application, which can be changed at any time by its manager, to an immutable decentralized application. Between these two spots lies a gradation of trust levels. Trust in the application governance members and in the change process in which the application is inserted are key to determine the trust level that a stakeholder has in a predicable execution of the application.

WHAT ABOUT THE TRUST FROM THOSE THAT ARE NOT PART OF THE GOVERNANCE STRUCTURE?

Besides the application governance, other stakeholders can endure the impact of changes in smart contracts. May this be the application users or the external observers, those people, referred to as stakeholders here, trust and believe that the smart contract is doing what it is supposed to do. The members of the governance structure are also stakeholders.

Having in mind that a specified code is immutable, the stakeholders can trust the compliance of the smart contract if they read and understood the code or if they believe that the application governance (or other stakeholders) made sure that the development of the smart contract conforms to the expected behavior.

Once there is a lot of effort involved in reading and understanding the code, one can assume that several stakeholders simply trust in the application governance. It is relevant to highlight that auditing or accredited institutions may be included in the application governance as to enhance its credibility.

For those stakeholders that do not trust the application governance and wish to analyze the immutable code in an independent manner, it is necessary to make sure that there is dependable mechanism to inspect the governance and the changes that might be made.

Is necessary to make sure that there is dependable mechanism to inspect the governance and the changes that might be made

The aforementioned automatized change process in the blockchain itself, which may increase trust among the governance members, may therefore increase trust among the stakeholders.

CHANGE PROCESS AND NETWORK LEGALITY

A change process in the decentralized applications is yet even more relevant for networks that intend to remain legal. Laws and regulations can change and turn smart contracts illegal if the immutable codes are not flexible enough to conform to changes that need to be made. An example of this would be a smart contract that calculates the total amount of taxes that need payment. What happens if one changes the rule of the calculation of the value? Besides that, court orders can determine that a smart contract needs a data change or even a code change. For instance, a court order can alter the parameter to calculate an alimony that needs periodical payment or also alter its calculation formula.

The absence of a mechanism for the application evolution makes it necessary to devise a solution that will effectively guarantee that the application remains legal. A way out is interrupting the execution of smart contracts and deploying new altered contracts by resorting to those responsible for defining and approving of new rules. This action can bring about (a) data migration issues and a possible loss of information, (b) an impact on external applications that depended on the modified application and (c) the stakeholders' loss of trust therein.

The absence of a mechanism for the application evolution makes it necessary to devise a solution that will effectively guarantee that the application remains legal

A more elaborate and bulkier solution would be having the application ready to an execution that is linked to a change process. Within this scope of change, just like the previous solution, one can also deploy new smart contracts, but that will take place within a known and traceable process, whose aim is maximizing trust among the stakeholders and minimizing the operational impact.

REQUIREMENTS FOR THE PROPOSED CHANGE PROCESS

This text will propose three high-level requirements for an application change process as follows. All of them must be met through on-chain development, so as to guarantee the predictability and trust of the process.

1. Facilitating the evolution of an application that uses smart contracts;
2. Providing the stakeholders with transparency in the change management process;
3. Ensuring that the application governance is in conformity with the application to be deployed or evolved.

The evolution of an application mentioned in item #1 can comprise correction of code error, update of some business requirements or change of the state variables of the contracts. Here are some examples of the facilitations that an application fitting the first requirement can offer, regarding an application change context: (a) preserving the access to the data used by the application, as a way to minimize data migration; (b) making it feasible to alter data in a way that was not meant by the business rules of the application; (c) making it feasible to alter the data structure, by preserving the access to the data used by the application; (d) exposing an immutable way of finding the current develop-

ment of the smart contracts; and (e) preserving the quality of the smart contracts codes throughout time, even after various evolutions.

According to the characteristics of a blockchain network, data stored in transactions for the network are not to be altered. It is only possible to alter the current state of the data stored in the variables of the smart contracts. Thus, the development of this item #1 is not able to solve the issue of the right to be forgotten present in privacy laws.

The second requirement (#2) grants the transparency in the process of change management. Besides meeting the first requirement, a development that conforms to the second one should: (a) establish that changes go through a life cycle, which involves specification, approval, execution and conclusion or cancelling; (b) associate the change with off-chain information that spells out for example its motivation and the rationale adopted for the solution; (c) make it possible to specify objectively, and preferably in an immutable fashion, the change script - so as to allow its analysis even before the change approval; (d) avoid the execution of changes that do not go through the change process; (e) provide transparency regarding which were the proposed changes and what happened to the these propositions and (f) work out a system to monitor the changes in progress.

Ideally, one should start discussing the change proposition in an off-chain way, in order to facilitate the debate and the evaluation of the impacts. Only when the members agree on what must be proposed should a change be proposed by using the process. In order to associate the change with the off-chain information (as described in item 'b'), it is possible, for instance, to register in the blockchain the hash that documents the motivation, discussion and the evaluation of the impact of the change and, possibly, the rationale adopted for the solution. A way to make the monitoring of the changes possible is (as described in item 'f') to emit an event for each modification of change state.

The last requirement aims at making sure that the stakeholders composing the application governance agree on the conformity of the smart contract. A development that meets the three requirements aforementioned must then have the concept of governance structure automatized, and it must be capable of deciding on changes in order to share the change responsibility. A voting mechanism can aid the group's decision-making process and the participants can be pointed out so that their responsibility transcends to real life as well. Developments can opt for classify changes in different levels of formality regarding deployment, which will depend on how high the change impact will be. One must also set out a rule concerning the inclusion or elimination of members of the application governance and one can form subgroups to vote on each change.

As previously discussed, the stakeholders must trust the decisions of the application governance group. It is important to highlight that the governance structure must be requested for since the very first deployment of the smart contracts so that they can be accounted responsible for it.

NOTES ON THE USE OF THE CHANGE PROCESS

A reasonable measure adopted in public networks governance is the you-are-free-to-opt-out principle (Lyons and Courcelas, 2020), which might occur at any time. The same measure applies to the application evolution. The change process as described have not included this as a mandatory requirement since the handling of this practice cannot be easily generalized to be dealt with out of the application code. Nevertheless, it is recommended that application governance assess and if possible support this practice in the specification of each change.

The change process does not take into account either that there can exist a time gap between the approval and the execution of the change, which would allow the stakeholders to take some time to decide what to do regarding the imminent application change as well as to develop an additional safety mechanism. It is necessary to discuss this possibility more thoroughly.
It is quite interesting to analyze an application by

observing the number and the criticality of the changes – the submitted, approved and executed ones. Several changes may imply constant changes of the business requirements or the spotting of flaws. By analyzing the information generated by the change process, any stakeholder can understand the history and the prediction of the application changes.

ANALOGIES WITH WELL-STABLISHED IT PRACTICES

The idea of design a tracking process, as well as formally deciding on changes is not new in IT service management. ITIL (Axelos, 2019) practices also include a change management process, in order to guarantee that the changes go through a pre-defined activity flow, involving assessment and approval. This aims at cataloguing and allotting the necessary measures to make changes, and if that is the case, to minimize the impact of potential incidents.

Regarding the application scenario in blockchain networks, the change process is also useful to make sure that the changes happen without a great trust impact on those who integrate the application governance and the stakeholders.

Development of the proposed change process – an example

The platform Ethereum does not natively offer support to the requirements described in this text, even though there may be some partial developments of the solution, such as that of the OpenZeppelin (OpenZeppelin, 2020), ERC1504 (Wu et al., 2017) and ERC930 (Lemble, 2018). A development proposition that partially implements those mentioned here can be found on https://github.com/bndes/Blockchain-ChangeManagementFramework.

An application development that uses the change management framework contains (a) smart contracts that are generic for the change process; (b) smart contracts created specifically for each change and (c) the very smart contracts of the application.

REFERENCES:

Axelos (2019), ITIL® Foundation, ITIL 4 edition. Disponível em: https://openzeppelin.com/.

Jimenéz, J. W. I (2020), Alastria Mission and Vision, A Multidisciplinary Research, Reus Editorial.

Lemble, A. (2018), ERC930 - Eternal Storage Standard, Ethereum Improvement Proposals. Disponível em: https://github.com/ethereum/EIPs/issues/930.

Lyons, T., Courcelas, L. (2020), Governance of and with Blockchains, EU Blockchain.

Observatory and Forum, Disponível em: https://www.eublockchainforum.eu/reports.

OpenZeppelin (2020), Upgrading Smart Contracts, OpenZeppelin docs. Disponível em: https://docs.openzeppelin.com/learn/upgrading-smart-contracts.

Werbach, K. (2018), The Siren Song: Algorithmic Governance By Blockchain, in After the Digital Tornado: Networks, Algorithms, Humanity. Disponível em SSRN: https://ssrn.com/abstract=3578610.

Wu, K., Ren, C., He R., Ma, Y., Liu, X. (2017), ERC-1504 Upgradable Smart Contract, Ethereum Improvement Proposals. Disponível em: https://eips.ethereum.org/EIPS/eip-1504

This framework is a working in progress. Please, get in touch if you are willing to contribute to this.

@Alastria_

JOIN US AND SHAPE THE FUTURE OF BLOCKCHAIN

Alastria is a semipublic, independent, permissioned and neutral Blockchain/DLT network, designed to be accordant with the existent regulation, that enables the associates to experiment these technologies in a cooperative environment.

As a member of Alastria, you will

Participate in growing the current Alastria infrastructures through the deployment of regular and/or validating nodes and in designing Alastria ID with a focus on making transactions on the networks with a legal validity.

Be part of a multi-sector blockchain ecosystem in which companies, experts, researchers, regulators and policy makers converge, with a relevant role in the DLT reference bodies in Spain, Europe and Latin America to actively shape the future of the industry.

Boost your organisation's innovation strategy, taking advantage of the dialogue between business, public administration and Academia to develop and generate new models of digital economy.

Become a member: alastria.io

ALASTRIA

Alastria Blockchain Ecosystem