Derechos reales y fintech: Cláusulas de garantías en la era cripto.

FACULTAD DE DERECHO
Autor: Teresa Miras Moraleda
Director: José María Elguero
ICADE 2025

Índice:

I. Introducción

II. Régimen jurídico: las criptomonedas y los derechos reales.

A. Breve explicación de las criptomonedas y el blockchain.

Debido a la complejidad de los conceptos que se van a manejar, y los mitos y dudas que los rodean, es menester empezar este trabajo con una explicación conceptual que se ajuste a nuestros propósitos. Sin vocación de ser minuciosa ni exhaustiva, esta sección hará un recorrido por el funcionamiento de una transacción con criptomonedas. El siguiente apartado repasará los hitos legislativos más relevantes sobre esta materia.

Al enfrentarnos a la enrevesada tarea de describir el funcionamiento de las criptomonedas, contamos con la ventaja de un claro punto de partida. En 2008, el enigmático Satoshi Nakamoto publicó un breve ensayo de ocho páginas titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (conocido en español como "El Libro Blanco del Bitcoin"). Este ensayo marcó un punto de inflexión en nuestra forma de entender las finanzas, materializando lo que hasta entonces solo habían sido teorías sobre la posibilidad de crear una moneda digital descentralizada. Mucho se puede divagar sobre la identidad de Satoshi Nakamoto. Escritores más versados sobre este asunto apuntan a la posibilidad de que se trate de un grupo de personas, o de alguna figura relevante del mundo del Fintech, pero ninguna teoría se ha podido probar, y el creador de Bitcoin elige permanecer en el anonimato. Lo único que parece claro sobre Nakamoto es su decisión de presentar al mundo su creación en el contexto de la crisis de 2008, un momento histórico en el que los ciudadanos habían perdido la confianza en los bancos, actores tradicionales del mundo financiero, y en el sistema económico en general.

La característica definitoria del bitcoin, la primera criptomoneda, más allá de ser una forma de pago digital, es su naturaleza descentralizada, capaz de garantizar la legitimidad de una transacción sin necesidad de un órgano supervisor. Este era el propósito de Nakamoto, que en su ensayo escribía: "Una versión puramente peer-to-peer (compañero-a-compañero) del dinero digital permitiría que los pagos online se mandasen de una parte a otra sin tener que pasar por una institución financiera."[1] El Bitcoin y el Blockchain nacen en el seno de movimientos neocapitalistas y cyberanarquistas, que rechazan abiertamente la intervención del

[1] NAKAMOTO, S. (2008) *Bitcoin: A peer-to-peer Electronic Cash System*. Editorial Bitcoin, UK. Disponible en: bitcoin.pdf

Estado e incluso la misma idea de un ente regulador con poder para intervenir en la esfera personal de los ciudadanos[2]. Sin duda estas ideologías han influido al propio diseño de estas herramientas de fintech, configurándolas de forma que eluden una regulación y supervisión clásica, o al menos dificultan gravemente la tarea. El propio Nakamoto expone como objetivo principal de su ensayo la creación de una moneda digital que no requiera de un tercero de confianza o institución financiera para validar las transacciones, pero que tampoco esté sujeto al código del honor como única garantía. La propia configuración de la tecnología de las criptomonedas está diseñada para resistirse a la supervisión y legislación.

El recorrido que vamos a realizar por el funcionamiento de la tecnología Blockchain y Bitcoin estará directamente informado por el siguiente párrafo, una transcripción traducida al español del ensayo de Nakamoto:

"Las **firmas digitales** proporcionan parte de la solución, pero los principales beneficios se pierden si un tercero de confianza sigue siendo requisito para evitar **problemas de doble gasto**. Proponemos una solución al problema de doble gasto utilizando una **red peer-to-peer.** La red sella la fecha y hora de las transacciones asociándolas a un **hash** dentro de una **cadena continua de proof-of-work (prueba-de-trabajo)** basada en hashes, creando un registro que no puede ser alterado sin rehacer el proof-of-work. La cadena más larga no solo servirá como prueba de una secuencia de eventos atestiguada, sino también como prueba de que proviene del **mayor grupo de poder CPU**. Mientras la mayoría del poder CPU esté controlado por nodos que no estén cooperando para atacar la red, generarán la cadena más larga y aventajarán a los atacantes. La red en sí requiere una estructura mínima. **Los mensajes se anunciarán en base al best effort** (mayor esfuerzo), y los **nodos** podrán marcharse y volver a unirse a la red a su voluntad, aceptando la cadena de proof-of-work más larga como prueba de lo acontecido durante su ausencia."[3]

Siguiendo la línea expositiva que propone Nakamoto, empezaremos analizando el funcionamiento de las firmas digitales, el hash y el problema del double spending. Luego profundizaremos en el funcionamiento del Bitcoin y de la red peer-to-peer (conocida como Blockchain), definiendo a su vez qué es el proof-of-work y su relevancia. Para asimilar esta

[2] Fonticiella Hernández, B. (2021). *La protección del inversor minorista en el panorama Fintech. Crowdfunding. Criptomonedas. Initial Coin. Offerings. (ICO)*. Editorial Dickinson.
[3] NAKAMOTO, S. (2008) Bitcoin: A peer-to-peer Electronic Cash System. Editorial Bitcoin, UK. Disponible en: bitcoin.pdf

información estudiaremos el proceso de una transacción de criptomonedas, cimentando todos los conceptos anteriormente descritos. Por último, analizaremos por qué argumenta Nakamoto que su red es segura a pesar de no contar con un ente supervisor. Todo esto nos ayudará a enfrentarnos a la pregunta de cómo configurar una cláusula de garantías para que sea válida a pesar de las particularidades de las criptomonedas.

1. Las firmas digitales, el Hash y el problema de double spending.

1.1 Las funciones criptográficas "hash"

Nakamoto define por primera vez la moneda que pretende crear como "una cadena de firmas digitales". Esta tecnología es de uso común desde hace años, pero su funcionamiento a menudo no es conocido. Para entenderlas, es necesario familiarizarse con el concepto de **funciones criptográficas "hash"** (CHF, en adelante). En esencia, los CHFs son algoritmos que codifican una serie de información (el input) usando una compleja transformación matemática, para obtener un único output que cumpla parámetros predeterminados que son característicos de cada CHF. El output se denomina más comúnmente "Hash". Es importante entender que, aunque el input pueda tener cualquier longitud, todos los Hashes producidos por un mismo CHF tendrán una misma longitud fija. Cada input puede corresponderse únicamente con un output. Estos algoritmos se denominan criptográficos porque todos los outputs producidos por un mismo CHF deben cumplir una serie de reglas (denominadas critical design choices) que los identifican como resultados de ese CHF, y permiten emplearlos para aplicaciones criptográficas.

Es decir, los CHFs son algoritmos que se usan para codificar sets de información que pueden reunir cualquier particularidad posible, convirtiéndolos en un número de longitud fija que cumpla unas características determinadas: el Hash. Los CHF son la base de numerosas aplicaciones, pero se emplearon por primera vez en las firmas digitales. MD5 y SHA-256 son los dos algoritmos CHF más comunes.

Para que un CHF se considere óptimo debe reunir unas características que más tarde serán relevantes. Primero, debe ser eficiente y no requerir mucho tiempo para producir el output. Segundo, debe ser muy difícil que dos inputs diferentes tengan el mismo output (esto se le denomina ser "collision resistant"). Tercero, el CHF debe anonimizar por completo el input, de forma que sea imposible saber cuál era el input partiendo del output; los Hashes no son decodificables ni reversibles. Por último, el output debe parecer aleatorio y no ser

predecible. Estas características no se pueden garantizar matemáticamente, por lo que una transacción nunca será completamente segura.

1.2 Las firmas digitales

Las firmas digitales, al igual que las firmas físicas, son una forma de vincular la identidad de una persona a un documento o transacción. Una operación con firma digital compone de cuatro elementos: la clave de firma (CF), la clave de verificación (CV), el mensaje y la firma (CFm).

Cada persona tiene una CF, que es privada y nadie más que el dueño debería conocer; y una CV, que es pública. Ambas son Hashes. Cuando el emisor quiere mandar un mensaje firmado, este se encriptará junto con la CF del emisor, través de la aplicación que gestione esa firma digital. El resultado será la firma (CFm): un Hash compuesto por el mensaje y asociado a la CF. La CFm garantiza que solo la persona con ese CF haya podido crear esa serie de números.

Como se ha explicado anteriormente, los Hash no son reversibles. Esta secuencia de números acompañaría al mensaje, porque de ella no se espera poder recuperar el mensaje original. Para verificar la firma, la plataforma que gestiona la firma digital introduce el mensaje, junto con Sm y la CV del emisor, en una transformación matemática que tiene como output "si" (la firma es válida, pues se corresponde con la CF del emisor, que solo el algoritmo conoce) o "no" (la firma no es válida). Por esta razón es necesario dos claves para cada persona: la CV es pública y permite verificar si el mensaje proviene del emisor, mientras que la CF es privada para que nadie más que el emisor pueda producir un Sm de esas características.

Como dice Nakamoto, podemos ver que las firmas digitales son una forma de verificar la identidad de una persona mediante medios digitales. Sin embargo, en este escenario aún existe un ente regulador (el algoritmo que verifica la firma) para dar validez a cada transacción.

1.3 El problema del Double Spending.

El doble gasto, como su propio nombre indica, es la acción de gastar una moneda dos veces, de forma que dos receptores distintos hayan recibido la misma moneda, y por lo tanto la moneda del segundo receptor sea una copia o duplicación de la primera moneda, y en consecuencia no sea válida. En el Bitcoin, esto es posible porque las monedas digitales no son

un bien material cuya posesión se pierde al entregarlo a otra persona, sino que son series de datos digitales (Hashes) que el emisor sigue teniendo incluso después de haberlo enviado a otra persona. Es decir, en realidad los Bitcoin no son fungibles. Este problema se suele solucionar mediante una actividad de policía por parte de un ente regulador, que comprueba todas las transacciones para asegurarse de que un emisor no transmita la misma moneda dos veces.

Las firmas digitales identifican y validan a usuarios dentro de una red, pero requieren de un algoritmo centralizado para validar cada transacción. El plan de Nakamoto es encontrar una forma de validar una transacción, asegurándose de que no se esté gastando una misma moneda dos veces, mediante una red peer-to-peer, creando un sistema donde el poder de legitimación pertenezca a la red, y no a un ente centralizado.

2. El Bitcoin, la red peer-to-peer y el proof of work:

2.1 El Bitcoin

Bitcoin, llevado a su esencia, es una cadena de firmas digitales, como si se tratase de un libro de registro donde cada persona que ha sido dueña de ese Bitcoin firma, en orden. Al final de la cadena se puede comprobar (mediante la firma digital) la identidad de la persona que es dueña del bitcoin ahora mismo. Cuando se hace una transacción, esta no deja de ser una declaración firmada digitalmente de que una parte quiere transferir cierto número de bitcoins, en su posesión, a la otra parte. La parte emisora es la que figura como parte receptora en la última transmisión registrada de ese bitcoin. La identidad de cada parte en el sistema se conoce a través de su CV.

Como el Bitcoin es asimilable a un libro de registros, y la forma de conocer la titularidad de un Bitcoin es saber la titularidad del receptor en la anterior transmisión, cada transacción de Bitcoin incluye datos de la transacción anterior. Esto crea una cadena de propiedad. Sin entrar en específicos sobre cómo funciona el algoritmo, el emisor creará una serie de Hashes vinculando los detalles de la transacción actual a los de la transacción anterior, de forma que cualquier operador de la red pueda verificar criptográficamente que el emisor era el legítimo propietario de esos bitcoins antes de la transacción, legitimando la cadena de propiedad. Como la transacción de los Bitcoin viene asociada a una CV, cualquiera que conozca la CV del emisor puede verificar que solo el emisor podría haber creado el Hash asociado a esa transacción, por lo que los Bitcoin le pertenecen.

Otra implicación de que cada transacción de Bitcoins deba estar vinculada a la transacción anterior es que los Bitcoin transferidos conjuntamente forman un "pack". Esto significa que solo puedo "gastar" cada transacción una vez. Si tengo veinte bitcoins de una única transferencia y quiero entregar diez, al hacer la transacción "gastaré" esos veinte bitcoins, pero solo transferiré diez al receptor, y me transferiré los diez restantes de vuelta. Ahora soy legítima dueña de esos Bitcoin en virtud de la transacción que acabo de hacer, y no de la transacción a través de la cual los obtuve originalmente. Si quisiese gastar cinco de los diez Bitcoins restantes, tendría que hacer lo mismo.

2.2 El Bloque y el Blockchain

Al realizar una transacción, la información de la misma se pasa a todos los usuarios (denominados "nodos") de la red. De estos usuarios, algunos serán mineros. Estos son los que se dedican a verificar que las transacciones son válidas y a añadirlas a un bloque con otras transacciones. Cada transacción en un bloque está codificada en función de las transacciones anteriores, de forma que al final todas las transacciones incorporadas a un bloque acaban resumidas en un único número. Los bloques no solo contienen las transacciones codificadas, también contienen un Hash identificativo, y *proof of work*, del que hablaremos más adelante. Cuando un minero consigue completar un bloque, lo hace público a la red. Si la red acepta ese bloque, el Hash identificativo, que codifica elementos informativos de ese bloque incluyendo el día y la hora, se unirá con el Hash del bloque anterior para sumarlo a la Blockchain. De esta forma, la cadena se hace más larga, y no puede ser interrumpida porque cada bloque está vinculado al anterior y al siguiente. La cadena más larga es la Blockchain legítima, porque es la que se ha verificado un mayor número de veces. En cualquier momento dado, la Blockchain debe poder seguirse hasta el bloque génesis.

El historial de transacciones es público, y solo existe uno. La clave del poder descentralizado del Blockchain es que existen múltiples cadenas, pero la única que se considera válida y legítima es la cadena que la mayor parte de usuarios de la red consideren válida y legítima, por ser la cadena intacta más larga que existe. Es decir, de cierto modo se democratiza el poder de decidir qué transacciones son válidas, confiando en que la mayor parte de los usuarios de la red sepan distinguir qué Blockchain es la correcta y estén actuando honestamente. Cuando un bloque se añade a la Blockchain, significa que la mayor parte de nodos de la red están de acuerdo con que las transacciones incluidas son legítimas. La aceptación se demuestra trabajando sobre ese bloque para crear uno nuevo.

2.3 Proof of work

El proof of work, resumido de la forma más sencilla posible, es como un acertijo que solo puede resolverse a base de prueba y error. Verificar la solución es fácil, pero conseguirla no lo es. No sirve otro propósito más que el de demostrar que una persona ha dedicado gran cantidad de esfuerzo a algo.

En Bitcoin, el proof-of-work que se debe dar es una serie de números que, al combinarlo en un algoritmo con la información del bloque que estén creando, se obtenga un numero con una cantidad determinada de ceros. Pasar ambos códigos por el algoritmo es rápido, pero conseguir el número que dé ese resultado solo puede hacerse mediante suerte, y prueba y error. Muchos nodos intentan conseguir un proof of work, por lo que de media se tarda diez minutos hasta que algún nodo tiene suerte y consigue el código correcto. Cada dos semanas se ajusta la complejidad del proof of work, para mantener la media de tiempo de resolución en diez minutos.

Al conseguir el proof of work, el nodo lo anunciará a la red. El resto de nodos descartarán el bloque en el que estuviesen trabajando y se pondrán a construir un nuevo bloque, aceptando el anterior como parte de la Blockchain y por lo tanto legitimando las transacciones contenidas en él. Las cadenas en las que los nodos estuviesen trabajando antes se descartan porque ya no son la cadena más larga, y por lo tanto, ya no son la Blockchain. Existe un sistema de recompensar a los mineros por su trabajo, que no detallaremos para no alargar esta explicación más de la cuenta.

El proof of work en informática se usa como una forma de evitar actuaciones malignas en una red, porque hace que imitar un bloque de la cadena requiera mucho esfuerzo. Dado que la única cadena válida es la más larga, una persona que tenga intención de añadir un bloque corrupto a la cadena debe conseguir crear un proof of work más rápido que el resto de nodos, que están colaborando para añadir a la cadena un bloque válido. Esto hace extremadamente difícil que la cadena pueda corromperse, siempre que la mayor parte de los usuarios de la red sean benignos, y que los “atacantes” no estén colaborando entre ellos para añadir el bloque corrupto. La creación de bloques legítimos siempre irá más rápido que la posibilidad de crear bloques falsificados. De esta forma, se sustituye la actividad de policía que antes llevaba a cabo el ente supervisor.

3. La transacción con criptomonedas

4. Cuestión de seguridad del Bitcoin

En base a lo que sabemos sobre el Bitcoin podemos afirmar varias cosas: primero, que para realizar una transacción de double spend, debes crear tu propio boque corrupto, porque los usuarios de la red podrán comprobar que ya habías transferido esos Bitcoin antes y nadie te validará la transacción; segundo, que para unir tu bloque corrupto a la Blockchain debes ser el primero en conseguir proof of work para ese bloque; y tercero, que estás compitiendo contra todos los usuarios de la red para crear ese proof of work, y por estadística es muy poco probable que consigas el proof of work más rápido que ellos. Siempre que los nodos honestos reúnan más poder que los nodos malignos que estén cooperando, es matemáticamente muy improbable que la cadena más larga no sea legítima.

Estas garantías también tienen que ver con las características de un Hash. Como hemos visto, casi todos los elementos de una transacción con blockchain son Hashes, desde las claves de los usuarios y el código de la transacción, hasta el código de la Blockchain y la forma de aprobar el proof of work.

5. Otros beneficios de la criptomonedas.

B. Régimen Jurídico de las criptomonedas

Para poder profundizar en la constitución de garantías sobre criptomonedas, primero debemos conocer nuestro punto de partida. A continuación, se realiza un recorrido por el actual régimen jurídico de las criptomonedas. La complejidad de esta tarea es patente, puesto que el marco normativo de estos instrumentos es disperso y se encuentra en pleno desarrollo. Por ello, el actual análisis se centrará en legislación específica a los activos digitales, junto con el marco de supervisión de actividades relacionadas con los criptoactivos, y concluirá con una reflexión sobre los retos y perspectivas de futuro de estos instrumentos de Fintech.

1. Legislación

Como se ha venido diciendo en el apartado anterior, la labor de legislar sobe criptomonedas es compleja, debido a su naturaleza descentralizada y a su concepción en el seno de movimientos ciber-anarquistas y neocapitalistas. A nivel nacional y europeo se han aprobado normas que intentan acotar en cierta medida los bitcoins, y empezar a establecer bases sobre las que constituir un régimen jurídico sólido. Sin embargo, el marco normativo que

les da soporte aún está en construcción, la regulación disponible es escasa y se presta a interpretaciones diversas.

La labor de legislar campos de innovación, como es la tecnología Fintech, debe ser un esfuerzo por preservar el equilibrio entre garantizar la seguridad jurídica, protegiendo los derechos de los ciudadanos y otros sujetos necesitados; y permitir suficiente espacio para que las tecnologías sigan desarrollándose y aportando a la sociedad. Por este motivo, la regulación que vamos a examinar puede ser básica, pero esto augura un buen desarrollo de las bitcoins en el futuro, y la posibilidad de que su uso se extienda.

1.1 Normativa Europea:

La Unión Europea es la fuente de gran parte de la legislación disponible respecto a criptoactivos, que trata de equilibrar la promoción de la innovación con la protección de los ciudadanos y de la estabilidad financiera de la zona euro. En los últimos años ha aprobado dos normativas principales con la intención de empezar a atacar el problema bitcoin. Estas son la Directiva AMLD5 y el Reglamento MiCA.

La **Directiva (UE) 2018/843 (AMLD5),** es la quinta directiva aprobada en materia de **la prevención del blanqueo de capitales y la financiación del terrorismo** e incluye, por primera vez, disposiciones aplicables a las criptomonedas. En particular, incorpora a los proveedores de servicios de intercambio de criptomonedas y custodia de monederos electrónicos (CASPs, por sus siglas en inglés) al ámbito de aplicación de esta directiva, exigiéndoles cumplir con medidas de Due Diligence; de identificación y verificación de clientes; y a reportar actividades sospechosas a las autoridades competentes. Esta inclusión también significa que los CASPs pueden ser sujetos a sanciones si incumplen sus obligaciones.[4]

El **Reglamento 2023/1114, sobre Mercados de Criptoactivos (Markets in Crypto-Assets Regulation,** o **MiCA)**, en vigor desde diciembre de 2024, responde a la necesidad de proporcionar una base legal armonizada para el tratamiento legal de los criptoactivos y sus proveedores en la Unión Europea, para proteger a inversores minoristas y generar confianza en los criptoactivos dando más seguridad a su mercado, previniendo conductas como el abuso de

[4] Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, 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.

mercado o el *insider trading*, y al uso de *wallets*. Se trata de una normativa integral sobre criptoactivos, que es pionero a nivel global al proporcionar un marco jurídico tan extenso[5]. Además, como resalta el Consejo General de la Abogacía Española, MiCA parece responder a las preocupaciones de que los criptoactivos puedan amenazar al control europeo sobre la política monetaria de la zona euro, debido a una volatilidad más que demostrada en eventos como los Tweets de Elon Musk, que impactaron la cotización de la moneda Bitcoin, creando una posible situación de abuso que podría poner en riesgo a los inversores minoristas[6].

El artículo 3 MiCA define los criptoactivos como "una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar." En el reglamento, están divididos en base a cómo estabilizan su valor, distinguiendo tres grupos: criptoactivos referenciados a activos, valores o derechos (con un valor vinculado a activos subyacentes), criptoactivos referenciados a monedas (los cuales buscan mantener un valor estable vinculado a una moneda de curso legal y se tratan de forma similar al e-money), y otros criptoactivos (categoría amplia que engloba, entre otros, las criptomonedas del estilo Bitcoin y Ethereum)[7]. Se deja intencionadamente fuera de su ámbito de aplicación a otras herramientas Fintech como los Non-Fungible Tolkens (NFTs) o el DeFi (Descentraliced Finance), que o bien cuentan con su propia legislación, o presentan particularidades tan significativas que requieren regulación propia. A pesar de sus limitaciones, Maria José Escribano, del equipo de Regulación Digital de BBVA, indica que "no puede negarse que MiCA es un paso muy importante para conseguir una adecuada protección de los consumidores así como para minimizar los riesgos que estos mercados son susceptibles de producir en la estabilidad financiera"[8].

---

[5] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937

[6] De la Mata, A. (20 abril 2023). *MICA. Aprobación del Reglamento de Mercados de Criptoactivos (MiCA). Necesidad de asesoramiento legal para un mercado en alza*. Consejo General de la Abogacía Española. Recuperado de: https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/mica-aprobacion-del-reglamento-de-mercados-de-criptoactivos-mica-necesidad-de-asesoramiento-legal-para-un-mercado-en-alza/ [Última consulta el 5/11/2024]

[7] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937

[8] BBVA. (20 abril 2023). *Regulación europea sobre mercados de criptoactivos (MiCA): qué es y por qué es importante*. Comunicaciones BBVA Recuperado de https://www.bbva.com/es/innovacion/regulacion-europea-sobre-mercados-de-criptoactivos-mica-que-es-y-por-que-es-importante/ [Última consulta 12/11/2024]

Como se ha establecido, MiCA trata de encontrar un equilibrio entre la seguridad jurídica y la innovación tecnológica, poniendo su foco en la expedición, oferta al público y admisión a cotización de criptoactivos, y de la prestación de servicios relacionados. Se establecen requisitos para la emisión de criptomonedas, su comercialización y la transparencia en su publicidad, reforzando la protección de los consumidores y creando un marco de supervisión para estas actividades. Además, impone obligaciones específicas para los CASPs que operan en la Unión Europea, entre las que se incluyen: ser una persona jurídica registrada como proveedor de servicios de criptoactivos en el registro oficial de algún Estado Miembro (aunque también se permite ejercer este rol a algunas entidades como a fondos de inversión alternativos, operadores de mercado de empresas de inversión o entidades de crédito); proporcionar y divulgar información completa y transparente sobre los criptoactivos que emitan, a través de un "libro blanco de criptoactivos", y responder por cualquier inexactitud de esta información; actuar de forma honesta, justa y profesional en el ejercicio de su actividad comercial y en el trato con sus clientes; disponer de garantías prudenciales dentro de unos estándares y valores mínimos establecidos; e implementar medidas de seguridad y cumplimiento de las normas de la AMLD5. Las obligaciones de los CASPs son moderadas en función del nivel de responsabilidad que asumen frente al cliente[9].

1.2 Normativa Nacional:

En España, no se reconoce a las criptomonedas como moneda de curso legal (por lo que no son un medio de pago oficial), sino como activos digitales susceptibles de ser poseídas, intercambiadas y empleadas en transacciones comerciales. La normativa española en este ámbito consiste mayoritariamente de transposiciones de la normativa europea anteriormente examinada.

La **Ley 10/2010, modificada por el Real Decreto-Ley 7/2021,** transpone la normativa AMLD5. A través de esta modificación se extienden las obligaciones legales de prevención del blanqueo de capitales a los CASPs. También se establece que el Banco de España mantendrá un registro de estas entidades, las cuales deben demostrar la idoneidad de sus directivos, y se

[9] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937

impone la obligación de cumplir con medidas de Due Diligence para la prevención de blanqueo de capitales mediante el uso fraudulento de estos activos financieros[10] [11].

Aunque la posición actual del Banco de España y la CNMV respecto de las criptomonedas es positiva, cabe mencionar que no siempre fue así. En 2018 estos órganos publicaron un comunicado conjunto en el que exponían su preocupación por la volatilidad de las criptomonedas y la facilidad de explotarlas como herramientas de abuso y fraude, recalcando que estas herramientas no son monedas de curso legal ni deben aceptarse como medio de pago oficial. Gran parte de las preocupaciones expresadas por estos órganos respondían a la falta de estructuras normativas y sistemas de regulación, obstáculos en vías de solucionarse. Como expresan en el comunicado: "Es esencial que quien decida comprar este tipo de activos digitales o invertir en productos relacionados con ellos considere todos los riesgos asociados y valore si tiene la información suficiente para entender lo que se le está ofreciendo. En este tipo de inversiones existe un alto riesgo de pérdida o fraude." [12]. Esta advertencia aún resuena hoy en día, en una sociedad donde el uso de criptoactivos se ha multiplicado, pero donde una gran parte de los inversores aún no saben las implicaciones de invertir en cripto, quedando además desprotegidos por una regulación y supervisión que empieza a existir, pero aún no está completamente desarrollada ni es lo suficientemente sólida para considerar a las criptomonedas una inversión segura.

2. Supervisión

Como se ha mencionado anteriormente, los criptoactivos generan preocupación entre inversores y supervisores, debido a la facilidad con la que se pueden emplear como herramientas de facilitación de fraude o blanqueo de capitales. Al abordar esta problemática es de particular relevancia el régimen de supervisión que tanto al UE como España han establecido. A continuación, veremos las entidades nacionales y europeas que trabajan

[10] Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

[11] Uría Menéndez. (9 de junio de 2021). *La modificación de la ley de prevención de blanqueo de capitales y financiación del terrorismo operada por el Real Decreto-Ley 7/2021 ¿Cómo afecta en la práctica?*. Circulares Uría Menéndez. Recuperado de https://www.uria.com/documentos/circulares/1417/documento/12353/Nota_clientes.pdf?id=12353 [Última consulta el 12/11/2024]

[12] Banco de España y CNMV. (8 de febrero de 2018). *Comunicado conjunto de la CNMV y del Banco de España sobre "criptomonedas" y "ofertas iniciales de criptomonedas" (ICOs).* Recuperado de: https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf [Última consulta: 20/01/2025]

coordinadamente para garantizar la protección de los inversores y el cumplimiento normativo en lo incumbente a las criptomonedas.

2.1 Supervisión a nivel nacional

El **Banco de España**, en virtud del Real Decreto Ley 7/2021 anteriormente mencionado, es el organismo que se encarga de la supervisión de os CASPs, con especial énfasis en la prevención de blanqueo de capitales y financiación del terrorismo. El Banco de España es uno de los órganos obligados a reportar actividades sospechosas a la Unión Europea. También es el órgano encargado de supervisar la emisión de criptoactivos vinculados a activos y criptoactivos vinculados a monedas de curso legal. Esta supervisión se lleva a cabo mediante inspecciones y auditorías, pudiendo imponer sanciones, medidas correctivas, o incluso suspender registros en caso de incumplimiento. Como principal medida de protección, el Banco de España mantiene un registro de CASPs, donde deben inscribirse todas las entidades que operen en España realizando actividades con criptomonedas o de custodia de *wallets*. Para registrarse, deben demostrar que cumplen ciertos requisitos establecidos en la legislación, de gobernanza corporativa y gestión de riesgos, además de proporcionar información detallada sobre sus actividades[13].

La **CNMV**, es el principal ente supervisor en materia de criptoactivos, centrándose en la protección de los inversores y la supervisión de Ofertas Iniciales de Monedas (ICOs), en actividades en las que los criptoactivos se emplean como instrumentos financieros. La CNMV también velará por el cumplimiento de las obligaciones establecidas en el MiCA, y resolverá conflictos relacionados con la protección de inversores. Además, se le consagra la colaboración internacional en materia de supervisión y regulación de criptoactivos, para promover la colaboración y mejores prácticas en este ámbito[14]. Con anterioridad su actividad en este ámbito estaba guiada por la Circular 1/2022, que fue derogada en 2024 con razón de la aprobación del

[13] Banco de España. (10 julio 2024). Aplicación del Reglamento relativo a los mercados de criptoactivos (MiCAR) respecto de la emisión de ART y EMT. Recuperado de: https://www.bde.es/f/webbe/GAP/Secciones/SalaPrensa/NotasInformativas/24/presbe2024-58.pdf [Última consulta 22/12/2024]

[14] CNMV. (s.f.). *MiCA: Nueva regulación de criptoactivos*. Recuperado de: CNMV - MiCA: Nueva regulación de criptoactivos. [Última consulta 22/12/2024]

MiCA, remitiendo a este para cualquier aspecto del trabajo de regulación de la CNMV en materia de criptoactivos[15].

2.2 Supervisión a nivel de la Unión Europea

El MiCA da un papel principal en la supervisión de los criptoactivos a la **Autoridad Europea de Valores y Mercados** (ESMA, por sus siglas en inglés), responsabilizándola de la supervisión directa de criptoactivos significativos de una forma similar a la supervisión que ejerce la CNMV en España. ESMA vigila los mercados de valores, y emite directrices sobre la regulación los criptoactivos cuando estos se emplean como instrumentos financieros. El objetivo último de este órgano es la protección del inversor, de la estabilidad en los mercados y de la transparencia, colaborando estrechamente con los órganos de supervisión nacionales para garantizar coherencia en su actuación y la correcta aplicación de las normas.

A la **Autoridad Bancaria Europea** se le encarga proporcionar directrices y recomendaciones para la gestión de riesgos asociados con criptoactivos, evaluando periódicamente su impacto en la estabilidad financiera de la zona euro. Es también una de las autoridades competentes en materia de prevención del blanqueo de capitales y financiación del terrorismo, en virtud de AMDL5.

3. Retos y perspectivas de futuro

Al evaluar la regulación y supervisión de las criptomonedas, es inevitable preguntarse sobre el futuro de estos activos. Su régimen jurídico está aún en pleno desarrollo, y aunque gracias al MiCA y otras iniciativas normativas se han empezado a dar pasos importantes hacia su regulación, aún quedan muchas incógnitas en el aire que abren la puerta a conductas innovadoras, y posiblemente fraudulentas, por parte de CASPs e inversores. La evolución tecnológica y el dinamismo e internacionalidad de estos mercados supone un desafío para los legisladores, que en este caso siguen a las nuevas tecnologías a varios pasos de distancia. Sin embargo, la prevención de estas actividades debe equilibrarse con permitir el desarrollo en Europa del mercado de criptoactivos, para no quedarse a la retaguardia del mundo en este aspecto.

[15] Circular 1/2024, de 17 de diciembre, de la Comisión Nacional del Mercado de Valores, por la que se deroga la Circular 1/2022, de 10 de enero, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión.

Las criptomonedas van camino de tener gran relevancia en diversos aspectos de nuestras vidas. Actualmente, el uso más popular para estas herramientas es el de instrumentos financieros, razón por la que sus principales órganos de regulación sean la CNMV y la ESMA, para la protección del consumidor. Sin embargo, su incidencia en el ámbito fiscal se empieza a ver claramente en como las autoridades fiscales de muchos países, incluyendo España, empiezan a moverse para gravar las actividades relacionadas con estos activos. El Derecho Penal también da pasos para la prevención del fraude en transacciones con criptomonedas. El papel que han jugados estas herramientas en la financiación de actividades ilegales no se puede pasar por alto, desde el caso Silk Road, una operación de compraventas ilegales y blanqueo de capitales financiada mediante Bitcoins[16]; hasta el caso Arbistar, una estafa piramidal a gran escala basada en criptomonedas[17].

Por último, otro ámbito en el que los criptoactivos están irrumpiendo, el que nos es realmente relevante, es en el derecho de propiedad y garantías. La posibilidad de constituir garantías sobre criptomonedas plantea importantes interrogantes jurídicos que este trabajo busca examinar. Se plantean como problemáticas principales la naturaleza digital descentralizada de las criptos y su falta de regulación específica, lo cual dificultan el embargo de estos bienes. En los próximos años la evolución legislativa en España determinará que dirección toma esta materia del derecho. Sin embargo, ya podemos empezar a especular al respecto, basándonos en los conocimientos que tenemos sobre esta materia en nuestro derecho, y la dirección que otros países, como Estados Unidos y Suiza, han tomado al respecto. Esta materia ocupará las siguientes partes del presente trabajo.

III. Las garantías sobre criptomonedas, en la teoría

A. Cómo constituir una garantía sobre criptomonedas

B. Cuáles serían las condiciones de contratación que se pueden establecer sobre esta garantía para hacerla rentable a bancos y otros acreedores

[16] Rasure, E. (24 de enero de 2025). *What Was the Silk Road Online? History and Closure by the FBI*. Investopedia. Recuperado de: https://www.investopedia.com/terms/s/silk-road.asp [Última consulta: 17/01/2025]

[17] Jiménez Sanchez-Mora, J. (22 abril 2021). *Caso Arbistar: la mayor estafa piramidal con criptomonedas. Economist&Jurist*. Recuperado de: https://www.economistjurist.es/economia/caso-arbistar-la-mayor-estafa-piramidal-con-criptomonedas/ [Última consulta: 17/01/2025]

IV. Las garantías sobre criptomonedas, en la práctica

A. Ejemplos prácticos de bancos que acepten criptomonedas como garantías y las condiciones de contratación que plantean

B. Como se ha venido tratando jurisprudencialmente el asunto

V. La problemática de las criptomonedas

A. Para los actores (falta de liquidez, volatilidad, falta de seguridad, asuntos de ciberseguridad y protección de datos…)

B. Para los consumidores (fragmentación del mercado de pagos, inseguridad sobre la posesión)

C. Para la sociedad (riesgo medioambiental, riesgo de fraudes)

VI. Conclusiones y propuestas