



## **FACULTAD DE DERECHO**

# **DERECHOS REALES Y FINTECH: Cláusulas de garantías en la era cripto.**

Autor: Teresa Miras Moraleda  
5º E3 B  
Área de Derecho Civil

Madrid  
Marzo 2025

## Índice:

<b>I. INTRODUCCIÓN</b> .....	3
<b>II. FUNCIONAMIENTO DE LAS CRIPTOMONEDAS</b> .....	5
1. LAS FIRMAS DIGITALES, EL HASH Y EL PROBLEMA DE DOUBLE SPENDING. ....	6
2. EL BITCOIN, LA RED PEER-TO-PEER Y EL PROOF OF WORK.....	9
3. LA CUESTIÓN DE SEGURIDAD EN BITCOIN .....	11
<b>III. RÉGIMEN JURÍDICO DE LAS CRIPTOMONEDAS</b> .....	12
1. LEGISLACIÓN EN ESPAÑA Y LA UNIÓN EUROPEA .....	12
2. SUPERVISIÓN NACIONAL Y EUROPEA .....	16
3. RETOS Y PERSPECTIVAS DE FUTURO .....	18
<b>IV. GARANTÍAS REALES Y CRIPTOMONEDAS</b> .....	19
1. GARANTÍAS REALES EN EL ORDENAMIENTO JURÍDICO ESPAÑOL.....	19
2. PROBLEMÁTICA DE LAS CRIPTOMONEDAS COMO OBJETO DE GARANTÍAS .....	27
<b>V. CLÁUSULA DE GARANTÍA SOBRE CRIPTOMONEDAS</b> .....	35
1. ESTABLECIMIENTO DE UN DEPÓSITO MEDIANTE CASPS.....	35
2. FIRMA DE UN PACTO MARCIANO .....	37
3. PACTO LOMBARDO Y CLÁUSULA LTV.....	38
4. PROPUESTA DE CLÁUSULA DE GARANTÍA SOBRE CRIPTOMONEDAS.....	39
<b>VI. CONCLUSIONES Y PROPUESTAS</b> .....	41
<b>VII. BIBLIOGRAFÍA</b> .....	45
<b>ANEXO I – Definiciones</b> .....	51

## I. INTRODUCCIÓN

La crisis financiera de 2008 estaba en pleno apogeo cuando, bajo el enigmático pseudónimo de Satoshi Nakamoto, se publicó en Internet un breve ensayo de ocho páginas titulado “*Bitcoin: A Peer-to-Peer Electronic Cash System*”. Esta obra cambió, de una pincelada, el panorama financiero global, presentando dos nuevas herramientas que permitirían cifrar e intercambiar monedas sin necesidad de la intervención de un ente tercero regulador. Las nombró Blockchain (Cadena de Bloques) y Bitcoin (Moneda de Bites), vocablos que pronto se integraría en el imaginario popular, aun cuando salta a la vista que la transversalidad de estas herramientas y su críptico funcionamiento sigue desconcertando a la mayoría. Mientras el mundo intenta adaptarse precipitadamente al fenómeno del Fintech, este continúa desarrollándose a una escala y velocidad de la cual aún no somos conscientes. El tres de enero de 2009 se minó el bloque génesis de Bitcoin, y actualmente se estima que más de 106 millones de personas son propietarias de esta criptomoneda. Bienvenidos a la era Cripto.<sup>1</sup>

Las criptomonedas son un valor y una forma de pago para muchas personas. Pero la inclusión del término “moneda” en su nombre induce a error, pues en poco se puede asemejar a las divisas más que en el hecho de que su valor es en realidad ficticio, derivado y vinculado a la confianza que sus usuarios depositan en ellas. El derecho, como disciplina que permea todos los ámbitos de nuestra existencia, ha tratado de dar respuesta a las criptomonedas, proporcionando seguridad a inversores y mineros, mientras trata de no impedir la innovación y el desarrollo. En este ingrato proceso, el Derecho ha encontrado grandes problemas para legislar sobre estos conceptos inmateriales. En este trabajo, ante la incapacidad de abarcar un asunto tan desbordante, centraremos la investigación en los derechos reales sobre criptomonedas, en particular el Bitcoin, y concretamente sobre un área del derecho de la contratación que está a la orden del día: las cláusulas de garantías.

No podemos ignorar que el Bitcoin y el Blockchain nacen en el seno de movimientos neocapitalistas y cyberanarquistas, que rechazan abiertamente la intervención del Estado e incluso la misma idea de un ente regulador con poder para intervenir en la esfera personal de los ciudadanos<sup>2</sup>. Sin duda dicha ideología ha influido en el propio diseño de estas herramientas

---

<sup>1</sup> Bitcoin. (s.f.). “The Bitcoin Revolution: How It All Started and Where We Are Now”. Bitcoin.com. <https://www.bitcoin.com/get-started/the-bitcoin-revolution/#:~:text=Explore%20the%20origins%20of%20Bitcoin%2C%20its%20impact%20on,regulatory%20andscape%2C%20and%20the%20future%20of%20digital%20currencies.>

<sup>2</sup> Fonticiella Hernández, B. (2021). *La protección del inversor minorista en el panorama Fintech. Crowdfunding. Criptomonedas. Initial Coin. Offerings. (ICO)*. Editorial Dickinson.

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. Es decir, la propia naturaleza de las criptomonedas está diseñada para resistirse a la supervisión y legislación. A pesar de esto, declarar a las criptomonedas una causa perdida no es satisfactorio ni suficiente para una realidad en la que esta tecnología se extiende con creciente rapidez.

El presente trabajo se compondrá de cuatro partes. En la primera desarrollaremos, basándonos en el ensayo de Nakamoto, una breve explicación del funcionamiento del blockchain y las criptomonedas. Luego revisaremos el régimen jurídico que se ha ido creando entorno a las mismas. En la tercera parte estudiaremos, desde una perspectiva teórica, la configuración de las garantías reales aceptadas en nuestro sistema jurídico y cuáles son los problemas que se plantean al intentar aplicarlas sobre criptomonedas. Por último, intentaremos dar solución a estos problemas empleando técnicas reconocidas y extendidas en nuestro ordenamiento jurídico, para concluir redactando una propuesta de cláusula de garantía sobre criptomonedas.

Antes de empezar, interesa hacer un aparte sobre el vocabulario empleado. Este trabajo contendrá bastantes tecnicismos, por lo que el Anexo I contiene definiciones de los conceptos más relevantes para facilitar la navegación por el presente texto. Además, por cuestión de claridad, “criptomonedas”, “cripto” y “bitcoin” se emplearán indistintamente para referirse al mismo fenómeno: las criptomonedas Bitcoin tal y como las presentó Nakamoto, ignorando las sutiles diferencias entre estos términos.

El presente trabajo tiene tres objetivos principales. El primero es entender el funcionamiento básico de las criptomonedas y su marco legislativo, para sintetizarlos y transmitir una imagen integral, si bien no minuciosa. El segundo es estudiar la teoría de las garantías reales con ayuda de dos libros jurídicos sobre derechos reales, para identificar las cuestiones que resultan problemáticas al establecer garantías reales sobre criptomonedas. El último objetivo es redactar una cláusula de garantía sobre criptomonedas que de solución a los problemas identificados anteriormente. Al terminar este trabajo espero haber reunido conocimiento sustancial sobre las criptomonedas y sus posibilidades, un área que actualmente

no domino; y a su vez haber afianzado mis conocimientos sobre garantías reales, al aplicarlos a la resolución de un problema práctico.

## II. FUNCIONAMIENTO DE LAS CRIPTOMONEDAS

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.

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.

Esto es relevante dado que 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 que perseguía Nakamoto, como declaraba en su ensayo: “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.”<sup>3</sup>

---

<sup>3</sup> Nakamoto, S. (2008) *Bitcoin: A peer-to-peer Electronic Cash System*. Editorial Bitcoin, UK. <https://bitcoin.org/bitcoin.pdf>

El recorrido que realizaremos 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.”<sup>4</sup>

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. 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 interno no es tan conocido. Para entenderlas, es necesario familiarizarse con el concepto de **funciones criptográficas “hash”** (CHF, en adelante). En esencia, los CHFs son algoritmos

---

<sup>4</sup> Nakamoto, S. (2008) *Bitcoin: A peer-to-peer Electronic Cash System*. Editorial Bitcoin, UK. <https://bitcoin.org/bitcoin.pdf> [traducción realizada por la alumna]

que codifican información (el input) usando una compleja transformación matemática, para obtener un único output que cumpla una serie de 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 (*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 ciertas características que más adelante serán relevantes. Primero, debe ser eficiente y no tardar mucho tiempo en 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 se pueden favorecer, pero no garantizar matemáticamente, por lo que una aplicación que emplee CHF nunca será completamente segura, pero puede aproximarse a un nivel de riesgo cero.

## **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 se compone de cuatro elementos: la clave de firma o firma privada (CF), la clave de verificación o firma pública (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 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 CFm y la CV del emisor, en una transformación matemática que tiene como output “sí” (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 CFm de esas características.

Como afirma Nakamoto, 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 (la aplicación 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 criptomoneda, y por lo tanto la moneda del segundo receptor no sea válida por ser una copia o duplicación de la primera. 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. En otras herramientas de Fintech, 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 mediante una red peer-to-peer, creando un sistema donde el poder de legitimación pertenezca a la red, y no a un ente centralizado. Será la propia red la encargada de evitar el *double spending*.

## 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 quién tiene la titularidad de un Bitcoin es saber la identidad del receptor en la última transacción realizada, cada transmisión 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 es el legítimo propietario de los bitcoins, legitimando así 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 alguien tiene veinte bitcoins de una única transferencia y quiere entregar diez, al hacer la transacción “gastará” esos veinte bitcoins, pero solo transferirá diez al receptor, y se transferirá los diez restantes de vuelta. Ahora esa persona es legítima propietaria de los diez Bitcoin en virtud de la transacción que acaba de realizar, y no de la transacción a través de la cual los obtuvo originalmente.

### 2.2 El Bloque y el Blockchain

Al realizar una transacción, la información de la misma se transmite 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 que pertenezca a 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 Hash. Los bloques no solo contienen las transacciones codificadas: para estar completos también deben contener un Hash identificativo, y el *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, dado que 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.

La clave del poder descentralizado del Bitcoin 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. Esta será la Blockchain. Es decir, en cierto modo se democratiza el poder de decidir qué transacciones son válidas, confiando en que la mayor parte de los usuarios de la red, actuando honestamente, sepan distinguir la Blockchain del resto de cadenas. 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 válidas. La aceptación de la red se demuestra cuando los mineros empiezan a trabajar sobre el último bloque añadido para crear uno nuevo. Para nosotros, la existencia de esta única Blockchain implica que el historial de transacciones es público, y que solo existe uno con legitimidad.

### **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 requiere mucho esfuerzo computacional (el poder CPU). No sirve otro propósito más que el de demostrar que una persona o grupo han invertido gran cantidad de poder CPU en resolverlo.

En Bitcoin, el *proof-of-work* que se debe proporcionar es una serie de números que, al combinarlo en un algoritmo con la información del bloque al que se corresponda, se obtenga un número con una cantidad determinada de ceros. Pasar ambos códigos por el algoritmo es

rápido, pero conseguir que el resultado cumpla determinadas características solo puede lograrse mediante prueba y error. En esta parte del proceso, muchos nodos trabajan simultáneamente, uniendo su poder CPU, para conseguir un *proof-of-work*, por lo que de media se tarda diez minutos hasta que algún nodo tiene suerte y consigue generar el código correcto. Aproximadamente 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 hasta entonces se descartan, porque ya no son la cadena más larga. Existe un sistema para incentivar y 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 añadir un bloque de la cadena requiera gran esfuerzo y dinero. Cuando la red actúa conjuntamente, combinando su poder CPU, este proceso se vuelve menos costoso para el individuo. Dado que la única cadena válida es la más larga, una persona que tenga intención de añadir un bloque corrupto debe conseguir crear un *proof-of-work* en solitario 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 honestos, y que los “atacantes” no estén colaborando entre ellos. 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 tradicionalmente lleva a cabo el ente supervisor.

### 3. LA CUESTIÓN DE SEGURIDAD EN BITCOIN

En base a lo que sabemos sobre el Bitcoin podemos afirmar varias cosas: Primero, que para realizar una transacción viciada (esto es, una transacción de *double spending*, en la cual un usuario pretende transmitir dos veces un mismo Bitcoin), el nodo deberá crear su propio bloque corrupto, porque si pidiese que la red verificase su transacción, los nodos podrían comprobar que ya habías transferido esos Bitcoin antes y ningún minero añadiría la transacción a su bloque. El bloque corrupto deberá contener las últimas transferencias realizadas, además

de la de *double spend*, y tendrá un Hash identificativo vinculado al del último bloque de la Blockchain. Esto significa que si un bloque se añade a la Blockchain durante este tiempo, el nodo maligno deberá empezar de cero.

Segundo, para unir el bloque corrupto a la Blockchain, el nodo maligno deberá conseguir *proof-of-work* para su bloque antes de que la red acepte un bloque nuevo, que haga que el corrupto devenga inútil. Como se ha indicado anteriormente, es matemáticamente improbable que un nodo actuando en solitario o con pocos cómplices sea capaz de obtener el *proof-of-work* más rápido que el resto de nodos de la red, que colaboran por verificar transacciones legítimas y reúnen la mayor parte del poder CPU. Solo si la mayoría de nodos de la red son malignos y actúan en colaboración puede existir un riesgo real de que se apruebe un bloque corrupto, y esta posibilidad es de nuevo altamente improbable, debido al esfuerzo que requiere en comparación con la poca rentabilidad que se obtendría.

### **III. 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 la legislación de estos instrumentos de Fintech.

#### **1. LEGISLACIÓN EN ESPAÑA Y LA UNIÓN EUROPEA**

Como se ha venido diciendo en el apartado anterior, la labor de legislar sobre 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 los 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 **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.<sup>5</sup>

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 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, previniendo conductas como el abuso de mercado o el *insider trading*. Se trata de una normativa integral sobre criptoactivos, que es pionera a nivel global por proporcionar un marco jurídico tan extenso<sup>6</sup>. 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

---

<sup>5</sup> 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.

<sup>6</sup> Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937

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<sup>7</sup>.

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). Se deja intencionadamente fuera de su ámbito de aplicación a otras herramientas Fintech como los Non-Fungible Tokens (NFTs) o el DeFi (Decentralized Finance), que o bien cuentan con su propia legislación, o presentan particularidades tan significativas que requieren regulación específica. 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”<sup>8</sup>.

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

---

<sup>7</sup> 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. <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/>

<sup>8</sup> BBVA. (20 abril 2023). *Regulación europea sobre mercados de criptoactivos (MiCA): qué es y por qué es importante*. Comunicaciones BBVA. <https://www.bbva.com/es/innovacion/regulacion-europea-sobre-mercados-de-criptoactivos-mica-que-es-y-por-que-es-importante/>

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<sup>9</sup>.

## 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). 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 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<sup>10 11</sup>.

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

---

<sup>9</sup> Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n° 1093/2010 y (UE) n° 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937

<sup>10</sup> 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.

<sup>11</sup> 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 y Uría Menéndez. [https://www.uria.com/documentos/circulares/1417/documento/12353/Nota\\_clientes.pdf?id=12353](https://www.uria.com/documentos/circulares/1417/documento/12353/Nota_clientes.pdf?id=12353)

las criptomonedas y la facilidad de explotarla como herramientas de abuso y fraude, recalando 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 responden 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.”<sup>12</sup>. 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 NACIONAL Y EUROPEA

Como se ha mencionado anteriormente, los criptoactivos generan preocupación entre inversores y supervisores, debido al uso que se les puede dar 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 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 los 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, y de supervisar la emisión de criptoactivos vinculados a activos y de 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

---

<sup>12</sup> 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)*. <https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf>

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<sup>13</sup>.

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<sup>14</sup>. 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 MiCA, remitiendo a este para cualquier aspecto del trabajo de regulación de la CNMV en materia de criptoactivos<sup>15</sup>.

## 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), responsable 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.

---

<sup>13</sup> Banco de España. (10 julio 2024). *Aplicación del Reglamento relativo a los mercados de criptoactivos (MiCAR) respecto de la emisión de ART y EMT*. Banco de España. <https://www.bde.es/f/webbe/GAP/Secciones/SalaPrensa/NotasInformativas/24/presbe2024-58.pdf>

<sup>14</sup> CNMV. (s.f.). *MiCA: Nueva regulación de criptoactivos*. CNMV. <https://www.cnmv.es/portal/mica/regulacion-criptoactivos.aspx?lang=es>

<sup>15</sup> 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.

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, el dinamismo y la globalización de estos mercados supone un desafío para los legisladores, que 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.

Las criptomonedas van camino de tener gran relevancia en diversos aspectos de nuestras vidas. Actualmente, un uso popular para estas herramientas es el de instrumentos financieros, razón por la que se encarga su supervisión a la CNMV y la ESMA. 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 jugado 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<sup>16</sup>; hasta el caso Arbistar, una estafa piramidal a gran escala basada en criptomonedas<sup>17</sup>, entre muchas otras.

---

<sup>16</sup> Rasure, E. (24 de enero de 2025). *What Was the Silk Road Online? History and Closure by the FBI*. Investopedia. <https://www.investopedia.com/terms/s/silk-road.asp>

<sup>17</sup> Jiménez Sanchez-Mora, J. (22 abril 2021). *Caso Arbistar: la mayor estafa piramidal con criptomonedas*. *Economist&Jurist*. <https://www.economistjurist.es/economia/caso-arbistar-la-mayor-estafa-piramidal-con-criptomonedas/>

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. Como problemáticas principales emergen la naturaleza digital descentralizada de las criptos y su falta de regulación específica, lo cual dificultan el embargo y ejecución de estos bienes. En los próximos años la evolución legislativa en España determinará que dirección toma esta materia del derecho. Sin embargo, podemos empezar a especular al respecto, basándonos en los conocimientos que tenemos sobre esta materia en nuestro derecho. Esta materia ocupará las siguientes partes del presente trabajo.

## **IV. GARANTÍAS REALES Y CRIPTOMONEDAS**

En esta sección analizaremos, desde una perspectiva teórica, la posibilidad de establecer cláusulas de garantías sobre criptomonedas. El presente trabajo está centrado en las garantías reales, por ser las que recaen sobre un bien (en este caso, las criptomonedas). Para realizar este análisis empezaremos detallando las características de las garantías reales, para luego identificar qué aspectos de las criptomonedas pueden ser problemáticos a la hora de poder ser objeto de garantía. Para concluir, propondremos cómo solventar dichos obstáculos y proporcionaremos un ejemplo de cláusula de garantía sobre criptomonedas. Como principal material de apoyo para elaborar esta sección se han empleado diversos capítulos de los libros “Derechos Reales (Tratado práctico interdisciplinar)” (Verda y Beamonte et al., 2023) y “Fundamentos del Derecho Civil y Patrimonial VI: Derechos Reales” (Díez-Picazo, 2012).

### **1. GARANTÍAS REALES EN EL ORDENAMIENTO JURÍDICO ESPAÑOL**

Los derechos de garantía son figuras jurídicas pertenecientes a los derechos reales, que permiten establecer un derecho de ejecución sobre un bien específico a favor de un acreedor. Su finalidad es vincular dicho bien al cumplimiento de una obligación principal, con el objetivo de proporcionar seguridad de que la deuda podrá satisfacerse, en caso de ser necesario, mediante la realización del valor del bien. Sirven, por lo tanto, como medida de refuerzo de un derecho: en caso de incumplimiento, el acreedor tendrá la potestad de instar la ejecución y enajenación de la cosa gravada por el derecho de garantía constituido, para satisfacer el crédito impagado con el valor de la misma. No se trata de una alternativa a la responsabilidad universal del deudor, del artículo 1911 del Código Civil (en adelante, CC), sino de una garantía añadida que establece un crédito privilegiado sobre el resto de acreedores. Es decir, con un derecho de garantía a su favor, el acreedor obtiene un derecho privilegiado que se antepone al de otros

acreedores del deudor, y a su vez un derecho de ejecución sobre un bien específico. Los derechos de garantía no confieren un poder inmediato sobre la cosa, sino un derecho preferencial de satisfacción patrimonial contra el valor de la misma, por lo que tienen un carácter accesorio respecto de la obligación que garantizan. Vienen regulados en los artículos 1857-1886 CC, como materia contractual, aunque Díez-Picazo apunta en el capítulo “XVIII: Los derechos reales de garantía” de su libro “Fundamentos del Derecho Civil y Patrimonial VI: Derechos Reales” (2012): “(...) la doctrina es concorde en calificarlos como derechos reales sin perjuicio de que tengan su origen en un negocio jurídico de carácter contractual”.

Las principales garantías reales en el derecho español son la hipoteca, la prenda y la anticresis. Cada una de estas modalidades tiene su normativa y funcionalidad particulares. En este trabajo nos centraremos en las dos primeras, pues la anticresis se constituye sobre los frutos de un bien, y las criptomonedas como las concebimos actualmente no generan frutos.

Las garantías reales cumplen una función económico-patrimonial esencial, permitiendo a los acreedores reducir el riesgo de impago y permitiendo a su vez a los deudores el acceso a financiación en condiciones favorables. Contribuyen pues a la seguridad del tráfico jurídico y el desarrollo de mercados financieros eficientes. La hipoteca ha jugado un papel fundamental en el mercado inmobiliario, permitiendo la movilización de financiación a gran escala que ha estimulado la inversión y adquisición de bienes inmuebles. Por su parte, la prenda ha permitido a empresas y particulares obtener liquidez sin tener que disponer de sus activos. Salta a la vista que las garantías reales son una herramienta esencial de nuestro sistema económico y jurídico, y un instrumento que debe adaptarse a las nuevas realidades del mercado, como son las criptomonedas. Sin embargo, su eficacia depende del marco jurídico y normativo que las respalda, por lo que cualquier irregularidad o incertidumbre puede desalentar su uso.

### **1.1 Principios generales de las garantías reales en España**

**Principio de accesoriedad.** Como ya se ha mencionado, un carácter esencial de los derechos de garantía es su accesoriedad, subordinación y dependencia de un crédito principal al que aseguran. Así viene establecido en el artículo 1857 CC: “Son requisitos esenciales de los contratos de prenda e hipoteca: 1.º Que se constituya para asegurar el cumplimiento de una obligación principal (...)”. Esta accesoriedad tiene varias implicaciones jurídicas. En primer lugar, la existencia de la garantía está directamente vinculada a la del crédito, y si este se anula o extingue, la garantía también se extinguirá automáticamente. En segundo lugar, para

transmitir la garantía es necesario ceder el derecho de crédito y viceversa. El nuevo titular del derecho de crédito lo será también de la garantía.

El artículo 1129 CC prevé la posibilidad de que el acreedor pueda anticipar la ejecución de la garantía o exigir prestación de nuevas garantías en caso de incumplimiento parcial de la obligación, riesgo grave de insolvencia del deudor, o por la existencia de circunstancias que hagan temer un menoscabo del bien sobre el que se establece la garantía.

**Principio de especialidad.** Es requisito esencial que tanto el crédito garantizado como el bien objeto de la garantía estén perfectamente determinados, para evitar que existan ambigüedades que puedan generar incertidumbre en el tráfico jurídico. Este principio va orientado a ofrecer seguridad a terceros interesados en la adquisición de bienes sobre los que existe o puede existir un gravamen, permitiéndoles conocer la extensión del mismo y las condiciones que podrían llevar a su ejecución. Es posible que una garantía recaiga sobre bienes fungibles, sujetos a transformación o sustitución, en cuyo caso deberá existir un mecanismo que asegure la permanencia del gravamen, por ejemplo, un registro.

**Principio de indivisibilidad.** Este principio, contenido en el artículo 1860 CC, establece que la garantía no puede fraccionarse. Esta no se reducirá si el deudor paga parcialmente el crédito, sino que subsistirá íntegramente hasta la satisfacción total del acreedor. El principio de accesoriedad visto anteriormente iba encaminado a proteger al deudor; y el principio de especialidad, a terceros interesados. Este principio se plantea como una protección de los intereses del acreedor, impidiendo que el deudor reduzca unilateralmente el alcance de su garantía hasta el punto de volverla insatisfactoria para cubrir la deuda. Cuando el acreedor quiera dirigirse contra el bien, podrá ejecutarlo en su totalidad y utilizar el valor para compensar la parte del crédito que permanezca insatisfecha. Una vez se extinga el crédito principal, el remanente se entregará al deudor o al resto de acreedores con derechos sobre el mismo bien.

**Prohibición de pacto comisorio.** El artículo 1859 CC establece que “El acreedor no puede apropiarse las cosas dadas en prenda o hipoteca, ni disponer de ellas.” Esto impide lo que se conoce como pacto comisorio, considerado un abuso por parte del acreedor por aprovecharse de la situación del deudor para hacerse con bienes cuyo valor supera el de la deuda garantizada. El acreedor deberá ejecutar el bien objeto de garantía mediante los cauces legales previstos, como la subasta mediante ejecución forzosa judicial o extrajudicial. De hacer

lo contrario, podría interferir con los derechos del deudor u otros acreedores de beneficiarse del posible remanente.

El pacto comisorio a menudo se confunde con la dación en pago. Este último es un mecanismo que permite al deudor saldar su deuda entregando el bien gravado, siempre que la entrega sea voluntaria y a posteriori del incumplimiento. Otra figura similar es el pacto marciano, que permite al acreedor quedarse con el bien objeto de garantía siempre que compense al deudor por la diferencia entre el valor del bien y el de la deuda. Es importante para que el pacto sea válido, que la valoración del bien se realice de forma objetiva y con garantías para el deudor.

## **1.2 Clasificación de las garantías reales en el derecho español**

A continuación, examinaremos distintos tipos de garantías reales en nuestro ordenamiento jurídico. Como ya se ha adelantado, nos centraremos en la prenda y la hipoteca. Existen tres supuestos de prenda especiales que estudiaremos por separado: la prenda sin desplazamiento, la prenda sobre derechos de crédito y la prenda irregular. En el caso de la hipoteca, distinguiremos entre hipoteca mobiliaria e inmobiliaria.

**Prenda.** Designamos como prenda al derecho real de garantía que recae sobre bienes muebles, y que se constituye mediante la entrega de los mismos al acreedor o a un tercero para su custodia, es decir, conlleva un desplazamiento de la posesión de la cosa pignorada. Existen casos específicos, que veremos a continuación, en los que por ley se permite un registro o una notificación como mecanismo sustitutivo del desplazamiento posesorio.

La prenda confiere al acreedor, además del derecho de ejecución y cobro preferente, anteriormente mencionado, el derecho de retención de la cosa. Este también lleva obligaciones asociadas: el acreedor deberá conservar la cosa con la diligencia de un buen padre de familia, respondiendo por su pérdida o deterioro si le es imputable. No podrá hacer uso del bien pignorado ni apropiárselo directamente, debido a la prohibición del pacto comisorio.

Puede ser objeto de prenda cualquier bien mueble que esté dentro del comercio de los hombres y sea susceptible de posesión. También puede recaer sobre ciertos derechos como créditos, acciones o títulos-valores, siempre que sean susceptibles de transmisión. Los bienes inmuebles quedan excluidos del ámbito de la prenda. El bien pignorado debe ser identificable

para cumplir con el principio de especialidad, excluyendo así la posibilidad de constituir garantías sobre bienes futuros (salvo casos tipificados) o de existencia incierta.

**Prenda sin desplazamiento.** Esta modalidad de garantía permite al deudor conservar la posesión de un bien pignorado, garantizando los derechos del acreedor y de terceros mediante una inscripción en el Registro de Bienes Muebles. Para realizar la inscripción, es necesario formalizar la prenda mediante escritura pública o póliza ante un fedatario público. Esta modalidad de prenda se utiliza para permitir que el deudor pueda seguir haciendo uso de la cosa pignorada, y para poder establecer prendas sobre activos cuyo desplazamiento posesorio es complicado, como frutos pendientes.

En este supuesto, dado que el deudor conserva la posesión de la cosa pignorada, debe someterse a un régimen de responsabilidad reforzado: además de deberes de conservación y cuidado, deberá recibir consentimiento del acreedor para disponer del bien. El acreedor podrá solicitar la ejecución de la garantía sin necesidad de entrega previa.

Los bienes susceptibles de ser objeto de prenda sin desplazamiento son *númerus clausus*. Se contienen en los artículos 52, 53 y 54 de la Ley, de 16 de diciembre de 1954, sobre hipoteca mobiliaria y prenda sin desplazamiento de posesión (en adelante, LHMPSD). Estos incluyen frutos pendientes, máquinas, mercaderías y materias primas almacenadas, derechos de crédito, y otros bienes cuyo desplazamiento posesorio es problemático. Dada la fecha de la norma en cuestión, huelga decir que esta enumeración no incluye a las criptomonedas.

**Prenda de derechos de crédito y valores negociables.** Este tipo de prenda sin desplazamiento posesorio no recae sobre bienes tangibles, por lo que tiene características particulares. La posibilidad se introduce en nuestro ordenamiento jurídico en 2007 como parte de la reforma del mercado hipotecario, pero se venía aceptando jurisdiccionalmente desde antes. El objetivo de este tipo específico de prenda es permitir al acreedor cobrar el crédito pignoraticio directamente de deudor del mismo. Por ello, bastará la notificación al deudor o depositario del crédito pignorado para la constitución de una prenda de derechos de crédito. Como indica José Ramón de Verda y Beamonte en su capítulo “Los derechos reales de garantía: la prenda” para “Derechos Reales (Tratado práctico interdisciplinar)” (2023), se trata más bien de la cesión de un derecho de crédito en garantía que de una garantía en sentido estricto, aunque existe gran debate doctrinal al respecto. Esta clase de prenda podrá constituirse sobre créditos comerciales, depósitos bancarios, derechos derivados de contratos y otros similares.

En el ámbito de las prendas de derechos de crédito, es pertinente también hablar del Real Decreto-ley 5/2005, de 11 de marzo, de reformas urgentes para el impulso a la productividad y para la mejora de la contratación pública, y en particular de su Capítulo II, que transpone la Directiva 2002/47, de 6 de junio de 2002, del Consejo Europeo, sobre acuerdos de garantía financiera. Este Real Decreto-ley introduce en nuestro ordenamiento un régimen simplificado de constitución y ejecución de garantías financieras entre profesionales que cambió por completo el mercado. Esta normativa es la primera en adoptar la constitución de garantías financieras mediante notificación, y la posibilidad de ejecución sin intervención judicial ni subasta pública, permitiendo que el acreedor se adjudique el bien garantizado de una forma similar al pacto marciano.

**Prenda Irregular.** Esta se constituye sobre bienes muebles fungibles, en general sobre dinero, permitiendo una autoliquidación de la deuda en caso de impago, eliminando la necesidad de recurrir a la ejecución forzosa. Un ejemplo típico es la fianza arrendaticia, esto es, un depósito que se le hace al arrendador y que al final del arrendamiento este utilizará para cubrir gastos de reparaciones imputables al inquilino, en caso de que sean necesarias, devolviéndole el remanente si hubiese. La característica esencial de esta prenda es esa imputación automática a saldar la deuda, sirviendo como una especie de pacto marciano o exclusión de la prohibición del pacto comisorio. La prenda irregular también permite que el acreedor disponga del objeto de la prenda, siempre que pueda devolverla en la misma especie y cantidad cuando el crédito sea satisfecho. Es importante señalar que el Código Civil no reconoce esta figura formalmente, y muchos autores la consideran en realidad un depósito o una autoliquidación, más que un derecho de garantía real. José Ramón de Verda y Beamonte, en su libro, señala: “Aunque, en este caso, hablamos de prenda, realmente no es tal, sino que estamos ante un mecanismo de autoliquidación de un derecho de crédito eventual, sin necesidad de acudir a un procedimiento de ejecución forzosa”.

**Hipoteca inmobiliaria.** Explicaremos esta figura brevemente en cuanto a que nos es relevante para comprender la hipoteca mobiliaria. Salta a la vista que el objeto de esta hipoteca no incluye criptomonedas, más no podemos dejar de mencionarla, pues es la garantía real más relevante de nuestro ordenamiento. Se caracteriza por constituirse sobre bienes inmuebles o determinados derechos sobre los mismos, y no requerir desplazamiento posesorio. Debe formalizarse en escritura pública e inscribirse, con todos sus datos, en el Registro de la Propiedad para tener eficacia frente a terceros. Viene regulada en la Ley Hipotecaria.

**Hipoteca mobiliaria.** Es posible establecer una hipoteca sobre bienes muebles, siempre que estos sean registrables en el Registro de Bienes Muebles. Al igual que la prenda sin desplazamiento, los objetos susceptibles de hipoteca mobiliaria son *númerus clausus*, y están contenidos en el artículo 12 LHMPD. Incluyen vehículos de motor, maquinaria industrial y derechos de la propiedad intelectual e industrial, entre otros, y excluye expresamente a los bienes que pueden ser objeto de prenda sin desplazamiento. La finalidad de esta figura es facilitar la obtención de financiación sobre bienes muebles de alto valor sin necesidad de perder su posesión.

En última instancia, parece que la principal diferencia entre la prenda sin desplazamiento y la hipoteca mobiliaria es, en la práctica, los objetos sobre los que se pueden constituir. Como reconoce Gema Reig Palmero, Registradora de la Propiedad, en su capítulo “La hipoteca mobiliaria y la prenda sin desplazamiento” para “Derechos Reales (Tratado práctico interdisciplinar)” (2023): “Para la división de prenda e hipoteca y para la determinación de los bienes muebles hipotecables, se ha seguido la distinción entre cosas muebles susceptibles de identificación registral y cosas muebles que no lo son. Estas últimas son las que en principio deben ser los objetos propios de la prenda común con desplazamiento posesorio. Más la extraordinaria variedad de la naturaleza física y del destino de las cosas muebles dificulta, o más bien imposibilita, la sumisión de todas a un tratamiento unitario”. Al describir la línea argumental que conduce a la delimitación del objeto de las prendas sin desplazamiento, los define como “bienes que no son susceptibles de ser hipotecados por su imperfecta identificación registral, tampoco lo son de prenda común por la imposibilidad física, jurídica o económica de su desplazamiento al acreedor o a un tercero”. Destaco la lógica expuesta por Reig Palmero porque tendrá implicaciones relevantes más adelante.

### **1.3 Constitución y ejecución de las garantías reales.**

Para constituir válidamente una garantía, es necesario cumplir con requisitos de titularidad y determinación. Primero, la persona que constituye la garantía sobre un objeto debe ser **titular** de la propiedad del mismo, o tener autorización legal para gravarlo en caso de pertenecer a un tercero. El deudor debe tener además libre disposición sobre sus bienes, o en su defecto estar autorizado para gravar dicho objeto. En caso de que la titularidad y propiedad de este bien se transmitiese por cualquier razón al acreedor, la garantía se extinguiría automáticamente por confusión. El objeto debe **estar determinado o ser determinable** en el

momento de la constitución, además de cumplir con los requisitos que cada tipo de garantía exige, evitando ambigüedades que pudiesen poner en riesgo la seguridad jurídica.

Además de estos requisitos, como ocurre con todos los derechos reales, las garantías deben tener alguna clase de **publicidad** para ser oponibles erga omnes. Si un tercero no ha tenido forma de conocer la existencia o impacto de un gravamen, este no podrá desplegar efectos más que sobre las dos partes que lo acordaron. En el caso de la prenda, basta la entrega del objeto como formalización, haciéndola oponible frente a terceros. Sin embargo, en los casos de la hipoteca y la prenda sin desplazamiento el derecho debe formalizarse en escritura pública o póliza ante fedatario público para poder inscribirlo en su correspondiente registro. Esta inscripción es constitutiva de la garantía, protegiendo los derechos del acreedor y de terceros interesados, y salvaguardando así la seguridad del tráfico jurídico. Como hemos visto anteriormente, existen casos en los que basta una notificación para constituir esta garantía. Estos mecanismos de publicidad son claves para determinar la existencia de derechos reales de garantía o incluso el orden de prelación entre los mismos, si se ha constituido más de uno sobre un mismo objeto.

Como última nota característica de las garantías es pertinente hablar de la **ejecución**, pues el principal valor de estas figuras jurídicas radica en poder oponer el valor de su objeto al pago de la deuda insatisfecha que garantiza. El acreedor dispone de varios mecanismos para hacer valer su derecho. La ejecución hipotecaria, judicial o extrajudicial, está regulada en los artículos 681 y siguientes de la Ley de Enjuiciamiento Civil, y consiste en una venta forzosa en subasta pública del inmueble. La adjudicación del bien al acreedor solo podrá acontecer si no acuden postores a la subasta, o no cumplen con su obligación de pago. En el caso de la prenda, el acreedor solicitará la venta pública en subasta, o la adjudicación del bien si existe pacto al respecto. Si se trata de una prenda sin desplazamiento, se estará a lo pactado por las partes, o en su defecto, a la venta en pública subasta. En el caso de una prenda sobre derechos de crédito, es posible el cobro del crédito o venta del valor en el mercado secundario, sin necesidad de subasta pública. Como medida de protección del deudor, este podrá librar al objeto pagando la deuda hasta el momento de la subasta o venta. Además, en caso de ejecución, tendrá derecho a cualquier remanente una vez el crédito haya sido satisfecho y no existan otros acreedores con privilegios especiales sobre el bien.

Concluido este breve estudio teórico de los derechos de prenda e hipoteca, procedemos a analizar su aplicabilidad a las criptomonedas, examinando las cuestiones problemáticas que se han hecho patentes a lo largo de este apartado.

## 2. PROBLEMÁTICA DE LAS CRIPTOMONEDAS COMO OBJETO DE GARANTÍAS

Las garantías sobre criptomonedas plantean problemáticas a tres niveles: su naturaleza jurídica y constitución, su compatibilidad con los principales tipos de garantía, y su proceso de ejecución. Vamos a analizar cada uno de estos puntos individualmente, sobre los cuales propondremos soluciones en el siguiente apartado de este trabajo.

### 2.1 Problemática de la naturaleza jurídica y constitución.

Carecemos de legislación nacional que nos permita determinar la naturaleza jurídica de las criptomonedas con exactitud. Lo único que podemos afirmar con certeza es que en ningún caso, bajo la normativa actual, se pueden considerar como monedas de curso legal, pues no están reconocidas como tales ni respaldadas por ninguna autoridad del mercado. A nivel europeo, podemos dirigirnos al MiCA para aportar cierta claridad. Como se examinó en la primera sección de este trabajo, el artículo 3 MiCA define los cryptoactivos 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.”

La doctrina de derecho privado española se encuentra inmersa en un debate al respecto de la naturaleza de las criptomonedas, sin haber llegado a una conclusión definitiva propuestas abarcan desde un derecho de propiedad intelectual hasta un contrato en soporte electrónico. Para nuestros fines, nos interesan las siguientes concepciones.

**Bitcoins como documentos electrónicos**, que pueden ser contraprestación en una transacción y son objeto de derechos reales. El Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS) define los documentos electrónicos en su artículo 3 como “todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.” Esta definición combina la concepción tecnológica de las criptomonedas con su posible uso jurídico. No es técnicamente incorrecta. Sin embargo, no se atiene a la verdadera esencia de las criptomonedas, ni se puede interpretar el eIDAS como un reglamento regulador de las mismas.

**Bitcoins como activos financieros.** Existe cierta similitud entre criptomonedas y acciones cotizadas expresadas mediante anotaciones en cuenta. Ambas representan, en su esencia, un registro de las personas que han ostentado la titularidad del mismo, hasta la última anotación que indica la titularidad actual. Ambas se negocian en un mercado, en el cual su valor fluctúa considerablemente en función de la demanda. Sin embargo, las acciones tienen a su vez la dimensión empresarial, dado que su propiedad tiene asociados ciertos derechos. Es posible, e incluso común, comprar criptomonedas para venderlas a un valor superior y obtener beneficios, de una forma similar a lo que se hace con acciones cotizadas y valores negociables. Pero no se puede afirmar que esto sea análogo a que las criptomonedas atribuyan a su titular un derecho financiero o de crédito, pues es necesario encontrar un comprador interesado, como señala José Francisco Sedeño López, investigador de la Universidad de Málaga<sup>18</sup>. Las acciones tienen una contrapartida en el capital social de una empresa, y en caso de extinción de la misma podrán reclamar esa cuantía (la cuota de liquidación). Al comparar las criptos con otros instrumentos financieros como bonos o derivados, se plantea lo mismo: al contrario que estos instrumentos, las criptos no cuentan con una figura de “deudor” a la que dirigirse para exigir la realización de su valor efectivo, más allá que recurrir a su venta en el mercado. Bitcoin no tiene una autoridad clara a la que reclamar si el sistema se hunde, pues ni siquiera conocemos la identidad de Satoshi Nakamoto ni de otros *Core Developers* y *Core Contributors* (los programadores que desarrollaron el software y lo mantienen activo)<sup>19</sup>. Cabe reiterar que Bitcoin no es una sociedad ni tiene un responsable al mando, es el producto de un software descentralizado de código abierto llamado Bitcoin Core<sup>20</sup>. Lo financian voluntarios y lo actualizan algunos programadores cualificados, sin ánimo de lucro, con ayuda de la comunidad.<sup>21</sup>

Aunque no encajan a la perfección con la figura de activos financieros, el Reglamento MiCA habla en múltiples ocasiones de la protección a inversores, y en España la CNMV es uno de los órganos supervisores de las criptomonedas, lo cual apunta a que los bitcoins si

---

<sup>18</sup> Sedeño López, J.F. (2020). *Naturaleza jurídica de las criptomonedas. Análisis de la STS de 20 de junio de 2019, rec. núm. 998/2018*. Revista de Contabilidad y Tributación. CEF, 442 (enero 2020), pp. 116-121.

<sup>19</sup> Bitcoin (s.f.) *Development* - Bitcoin. <https://bitcoin.org/en/development#bitcoin-core-contributors>

<sup>20</sup> Ashford, K. (21 mayo 2024). *What is bitcoin and how does it work?*. Forbes Advisor. <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-bitcoin/>

<sup>21</sup> Rothrie, S. (22 mayo 2020). *Who Controls Bitcoin? A Guide to BTC Stakeholders*. Crypto Briefing. <https://cryptobriefing.com/who-controls-bitcoin-guide-btc-stakeholders/>

pueden ser considerados instrumentos financieros. Sin embargo, para el objeto de este trabajo esta no es la concepción más adecuada.

**Bitcoins como medio de pago.** El notario Víctor J. Asensio en su artículo “El Bitcoin: una primera aproximación jurídica en derecho civil español” (2019), examina la equiparación de las criptomonedas a monedas tradicionales. Defiende esta postura basándose en la STJUE, de 22 de octubre de 2015, David Hedqvist, asunto C-264/14 la cual declara que el bitcoin “constituye un medio de pago directo entre los operadores que la aceptan”. Esta definición es interesante, puesto que permitiría emplear las monedas como medio de pago, calificando sus transacciones como compraventas en vez de permutas. Aunque no la menciona, también la STS 326/2019, de 20 de junio de 2019, se inclina por esta concepción, declarando que los bitcoins se pueden considerar “como un activo inmaterial de contraprestación o de intercambio en cualquier transacción”, aunque en la misma sentencia los denomine “bienes inmateriales” y reitera que no se pueden equiparar a una moneda de curso legal. Asensio reitera que el hecho de que no hayan sido aceptadas como moneda de curso legal no impide que se utilicen como tal<sup>22</sup>. Raúl Ruiz Rodríguez, investigador de la Universidad de Alicante, argumenta lo contrario, destacando que no se puede considerar “dinero” a aquello que no ha sido reconocido oficialmente como tal, y que la falta de respaldo oficial y supervisión hace que no concurren en las criptomonedas los rasgos característicos de una divisa<sup>23</sup>. En cualquier caso, no debemos dejar de recordar que el valor de los medios de pago procede de una aceptación generalizada de que tienen valor como medios de pago.

La naturaleza fungible de las criptomonedas también es discutible. El artículo 337 CC describe los bienes fungibles como “(...) aquellos de que no puede hacerse el uso adecuado a su naturaleza sin que se consuman.” El consenso general es que los bitcoins cumplen este requisito, pero esta cuestión cabe ser examinada en más profundidad. La propiedad de los Bitcoin viene dada por un hash en el cual se transmiten una cantidad de criptomonedas particular. Para volver a transmitir estas criptomonedas, es necesario “consumir” este hash por completo y generar uno o varios nuevos. Las criptomonedas persisten en el mismo número y calidad que antes de la transacción, sin embargo, se hace evidente que, de cara a realizar una transferencia, la identidad de la moneda individual es relevante en la medida en la que está

---

<sup>22</sup> Asensio Borrellas, V. (5 julio 2019). *El bitcoin: una primera aproximación jurídica en derecho civil español*. Lefebvre: El Derecho. <https://elderecho.com/bitcoin-una-primer-a-proximacion-juridica-derecho-civil-espanol>

<sup>23</sup> Ruiz Rodríguez, R. (2020). *Las criptodivisas como medio de pago y el Derecho internacional privado*. CUADERNOS DE DERECHO TRANSNACIONAL, 12(2), 740-757. <https://doi.org/10.20318/cdt.2020.5628>

asociada a un título de propiedad concreto. La cuestión es compleja, más dado que el consenso general es que se trata de bienes fungibles por su equiparación con las monedas, los consideraremos como tales en adelante.

**Bitcoins como bienes inmateriales digitales.** Esta concepción, al igual que la de medio de pago, está ampliamente aceptada en nuestro sistema jurídico. Tanto el Tribunal Supremo<sup>24</sup> como la Dirección General de Tributos<sup>25</sup>, en 2019 y 2018 respectivamente, han calificaron las criptomonedas como bienes inmateriales susceptibles de propiedad. Actualmente no existe una manifestación física de las criptomonedas, ni están registradas oficialmente por una autoridad del mercado. Ser un bien inmaterial significa que las criptomonedas son susceptibles de disposición, propiedad, y valoración económica, entre otras cosas.

La novedad de los bitcoins en comparación con otros bienes inmateriales, según Asensio, reside en que su sistema de transmisión y apropiación es único. Este autor llega a plantear si no debería crearse una nueva categoría jurídica para estos instrumentos. Tras su análisis del sistema Blockchain, concluye que los bitcoins son bienes susceptibles de propiedad, de transmisión personalísima (pues solo la puede realizar su titular), con contenido patrimonial, y su propio sistema de normas (el código fuente de Bitcoin), pero sin ninguna autoridad que supervise su cumplimiento (más allá del sistema detallado en el primer apartado de este trabajo).

Las diferentes perspectivas analizadas reflejan la dificultad de definir una naturaleza jurídica exacta para las criptomonedas en nuestro sistema, y es probable que no exista consenso hasta que una autoridad jurídica se pronuncie definitivamente al respecto. Para este trabajo, continuaremos explorando las garantías sobre criptomonedas considerando a las mismas como un medio de pago y bien inmaterial, pues son las definiciones que mejor se ajustan a nuestros propósitos.

El siguiente problema que se nos plantea es la **identificación y determinación** de las criptomonedas. Que existan únicamente garantizadas por el sistema de Blockchain hace que tengamos que recurrir a medios especiales para ello, puesto que ni existen en forma física, ni están registradas o garantizadas por una autoridad central. Por ello, a la hora de constituir una garantía va a ser necesario llevar a cabo una individualización y determinación de las

---

<sup>24</sup> Sentencia Tribunal Supremo, Sala de lo Penal, nº326/2019, de 20 de junio de 2019

<sup>25</sup> Resolución Vinculante de Dirección General de Tributos, V1149-18, de 08 de mayo de 2018

criptomonedas gravadas por la garantía, salvo que optemos por establecer una prenda irregular. La cuestión de **titularidad y disposición** de la criptomoneda también puede ser compleja. A priori, como hemos dicho, la titularidad es pública, y no tendríamos más que dirigirnos a la Blockchain para conocerla. La cuestión se complica al examinar la disposición: solo aquella persona que tenga la clave privada del titular del bitcoin podrá disponer del mismo. Esto tiene tres implicaciones: primero, que las criptomonedas no se podrán enajenar sin esta clave; segundo, que no hay forma de impedir que el titular transfiera las criptomonedas a otra persona, puesto que no hay forma de publicitar a terceros que estas están gravadas, y una vez se haya realizado la transferencia esta es irrevocable; y tercero, que cualquier persona ajena al titular que tenga dicha clave podrá disponer de los bitcoins. Tendremos que idear una forma de permitir la enajenación de las criptomonedas y prevenir que el titular o un tercero disponga de ellas hasta que el crédito esté satisfecho.

## 2.2 Problemática de compatibilidad con los tipos de garantías

Comenzaremos examinando la falta de idoneidad de la **hipoteca** como forma de garantía sobre criptomonedas. El principal problema de esta figura reside en que las criptomonedas no están legalmente aceptadas como objeto de la misma. La hipoteca inmobiliaria queda descartada por, válgase la redundancia, no ser las criptomonedas un inmueble. La hipoteca mobiliaria, por otra parte, es una figura cuyo objeto es numerus clausus delimitado en la LHMPSD, como ya se ha examinado, y no abarca los bitcoins ni ninguna figura que se le asemeje lo suficiente para establecer analogía. El supuesto más cercano contemplada por el artículo 12 LHMPSD son los derechos de propiedad intelectual. Es cierto que algunos autores han intentado plantear que las criptomonedas se pueden calificar como tales. En una de las primeras aproximaciones a la naturaleza de las criptomonedas a nivel global, “*Bitcoin: A First Legal Analysis - with reference to German and US-American law*”, las juristas alemanas Franziska Boehm y Paulina Pesch plantean subsumir esta figura al ámbito de aplicación de la Ley de Copyright alemana (Urheberrechtsgesetz) pues contiene normas especiales relativas al software. Sin embargo, ellas mismas descartan esta concepción por no ser las criptos el resultado de una actividad creativa ni tampoco un software propiamente dicho, sino más bien un resultado del mismo<sup>26</sup>. Además, al contrario que los derechos de propiedad

---

<sup>26</sup> Boehm, F y Pesch, P. (2014). *Bitcoin: A First Legal Analysis - with reference to German and US-American law*. University of Münster.  
<https://www.zar.kit.edu/downloads/Publikationen/Franziska%20Boehm/BTC%20final%20camready.pdf>

intelectual, las criptos no cuentan con un sistema de registro oficial que permita su identificación individualizada ni su entrada en el Registro de Bienes Muebles.

La idoneidad de la **prenda** es cuestión diferente, puesto que esta figura nos ofrece un abanico más amplio y flexible de posibilidades. Considerando las criptos como bienes muebles intangibles, podrían ser en teoría objeto de esta figura. El primer problema que se plantea es el desplazamiento posesorio, pues como se ha delimitado anteriormente, solo la persona con las claves privadas del titular del bitcoin puede realizar su transferencia. Además, dado que las transacciones mediante Blockchain son irreversibles, transferirlas al acreedor tampoco parece una solución ideal, puesto que no se puede separar la posesión de las criptos de su propiedad, y al recibir el acreedor la propiedad de los bienes objetos de garantía, esta se extinguiría por confusión. Además, esto supondría un incumplimiento de la prohibición de pacto comisorio. Establecer una prenda sin desplazamiento tampoco parece posible, puesto que las criptomonedas no están contempladas dentro de su objeto tasado en la LHMPSD.

Recurriendo a tipos alternativos de prenda, planteamos la posibilidad de establecer una configuración similar a la **prenda sobre derechos de crédito**. Esta solventa algunos de los problemas anteriormente mencionados: no es necesario que exista traslado posesorio físico ni registro oficial, puesto que se formaliza con una notificación al deudor; y recae sobre bienes intangibles, como son las criptomonedas. Además, la posibilidad de ejecutarlas extrajudicialmente, sin subasta pública, vendiéndolas directamente en el mercado secundario, nos es muy interesante en el ámbito de las criptomonedas. Vuelve a plantearse la problemática de su naturaleza jurídica: la posesión de un bitcoin no genera un derecho de crédito a favor del titular. Un crédito tradicional, una acción, un bono u otras figuras análogas cuentan con una entidad o persona vinculada a pagar al titular un respaldo, ya sea en satisfacción de una deuda, una cuota de liquidación o un reembolso. Las criptomonedas no tienen valor más allá del que el mercado le atribuya, por lo que no encaja perfectamente con la concepción de un derecho de crédito.

Si consideramos las criptomonedas como medio de pago fungible, no podemos dejar de plantearnos la posibilidad de establecer una **prenda irregular**, figura que también permite una ejecución ágil de la garantía. Sin embargo, volvemos a encontrarnos con el problema del traslado posesorio, dado que la propiedad y la posesión de las criptomonedas son inseparables.

## 2.3 Conclusiones

Los obstáculos al considerar las criptos como objeto de garantía son reiterativos, surgiendo una y otra vez en diferentes ámbitos de la investigación que acabamos de realizar. Utilizaremos este apartado para unificarlos antes de proceder a exponer nuestra propuesta de cláusula de garantía sobre criptomonedas que los solvente.

El primer problema es relativo a la **identificación, determinación y disposición de las criptomonedas**. Las criptomonedas son un bien generalmente considerado fungible, por lo que para establecer una garantía sobre estas debemos o bien encontrar una forma de volverlas específicas y determinadas, como puede ser la entrega; o bien emplear una forma de garantía que prevea ser constituida sobre bienes fungibles, como la prenda irregular. Además, por la naturaleza de las criptomonedas y de las claves privadas, también habrá que encontrar una forma de asegurar que la persona o entidad que tenga titularidad sobre las criptomonedas durante el término de la garantía no pueda disponer de ellas.

La siguiente cuestión es la **constitución válida de la garantía**. Salvo que recurramos a prendas con características especiales, existen dos formas de publicitar una garantía para que su constitución se considere válida y oponible erga omnes: el desplazamiento posesorio o la inscripción en un registro. La primera opción resulta muy problemática con las criptomonedas por su mecanismo único de transmisión, que no permite separar la posesión de la propiedad dentro de la red de Blockchain. Si se trasladan las criptomonedas al acreedor, la garantía se extinguirá por confusión y además se podría estar infringiendo el pacto comisorio. En cuanto a la segunda opción, las criptomonedas no son en la actualidad inscribibles en el Registro de Bienes Muebles ni en ningún otro análogo con validez en España, por lo que no podemos apoyarnos en la publicidad registral para la constitución. Además, la Blockchain no cuenta con ningún mecanismo que permita inscribir y publicitar gravámenes ni límites a la propiedad de los Bitcoin, por lo que nos preocupa también la protección de terceros, que no tienen forma de conocer si las criptos que van a adquirir están gravadas por una garantía

Además, como se ha examinado extensamente, las criptomonedas **no encajan idóneamente en ninguno de los tipos de garantías reales reconocidos en nuestro sistema**. El problema del desplazamiento posesorio impide que sean prendas ordinarias ni irregulares. No están incluidas en la enumeración *numerus clausus* de objetos de la prenda sin desplazamiento ni la hipoteca mobiliaria, ni son inmuebles sobre los que se pueda establecer

una hipoteca inmobiliaria. Tampoco proporcionan un derecho de crédito, por lo que no puede establecerse como una garantía sobre derechos de crédito.

La cuarta cuestión que nos preocupa es el asunto de la **ejecución de la garantía**. Este problema ha ido resonando a lo largo de todo el trabajo: son necesarias las claves privadas del titular para disponer de los bitcoins, pero no podemos pedir al deudor que nos proporcione sus claves privadas porque esto supondría un abuso: nos daría disposición sobre todas sus criptomonedas, no solo sobre aquellas objeto de la garantía. Sin embargo, sin estas claves los bitcoins son inembargables, pues no existe ningún mecanismo para disponer de ellos sin la clave, ni autoridad a la que podamos dirigirnos para exigir su ejecución. Además, la forma más directa de realizar el valor de un bitcoin es mediante su venta en el mercado de bitcoins, por ser este un mercado abierto y transparente. La ejecución forzosa en pública subasta no es un método ideal para ello.

El anterior problema plantea a su vez la última cuestión: la **volatilidad del valor de las criptos**. Los acreedores asumen un riesgo significativo al aceptar una criptomoneda como garantía, pues son activos cuyo valor fluctúa enormemente. En el caso de los Bitcoin, su variación se mide diariamente en función de la demanda del mercado, y suele rondar el 3% diario. El 23 de enero de 2025 un Bitcoin equivalía aproximadamente a \$103k, el 23 de febrero equivalía entorno a \$96k y el 23 de marzo entorno a \$83k, lo cual supone una depreciación de más de veinte mil dólares en tres meses<sup>27</sup>. La criptomoneda se encuentra actualmente en una tendencia descendiente, pero históricamente también ha aumentado su valor con rapidez: en noviembre de 2024 subieron en valoración de \$67k a \$98k en seis días, por la victoria de Donald Trump, conocido partidario de las criptomonedas, en las últimas elecciones estadounidenses<sup>28</sup>. Las noticias están plagadas de desplomes y subidas muy llamativos del valor de Bitcoin. En 2013 se dio una caída del 81% tras el desmantelamiento de la red criminal Silk Road (anteriormente mencionada), y más recientemente en 2024 una caída del 37% cuando la Comisión de Bolsa y Valores de Estados Unidos (SEC) interpuso una demanda contra varias criptomonedas, entre las cuales no se incluía Bitcoin<sup>29</sup>. La conclusión que

---

<sup>27</sup> CoinGlass. (s. f.). *Bitcoin historical volatility*. Coinglass. <https://www.coinglass.com/es/pro/i/bl>

<sup>28</sup> Macheel, T. (29 noviembre 2024). *Bitcoin heads for nearly 40% November gain as it edges closer to \$100,000*. CNBC. <https://www.cnbc.com/2024/11/29/bitcoin-heads-for-nearly-40percent-november-gain-as-it-edges-closer-toward-100000.html?msockid=13e44d9df04967351bd95e10f18a6655>

<sup>29</sup> Amelia. (s.f.). *10 Biggest Falls in Bitcoin History: Bitcoin's Biggest Crashes*. The Network Journal. <https://tnj.com/biggest-falls-in-bitcoin-history/>

extraemos es que no se puede asegurar con las criptos una cuantía suficiente para cubrir la deuda, pues el valor puede haberse desplomado antes de que ejecuten la garantía. Lo contrario también puede ocurrir: un enorme incremento en el valor de los bitcoins hará que el deudor no pueda disponer de esa riqueza, que sobrepasa significativamente el valor del crédito garantizado.

## **V. CLÁUSULA DE GARANTÍA SOBRE CRIPTOMONEDAS**

Hemos ideado una cláusula de garantía sobre criptomonedas que da solución a todos los problemas expuestos anteriormente. Para su elaboración, nos hemos inspirado en las prendas sobre créditos, puesto que ofrecen las condiciones de ejecución más favorables, y la constitución que mejor encaja con el funcionamiento de las criptos. Sin embargo, los bitcoins no son subsumibles a ninguna de estas dos formas de garantía. Por ello, partiremos de la base de una prenda ordinaria, configurando cláusulas que introduzcan una serie de cambios y adaptaciones que permitan establecer las condiciones más favorables para el acreedor, respetando también la protección del deudor y de terceros, y la legislación vigente. Estas son: una cláusula de establecimiento de depósito mediante CASPs, una cláusula de pacto marciano, y una cláusula LTV.

### **1. ESTABLECIMIENTO DE UN DEPÓSITO MEDIANTE CASPS.**

La regulación existente sobre criptomonedas, más específicamente el MiCA y sus transposiciones, está centrada en los CASPs, imponiéndoles obligaciones de registro (en nuestro país, con el Banco de España), de información a inversores, de ser garantes de seguridad y de actuar con profesionalidad en los términos establecidos en el reglamento. Hemos revisado estas obligaciones al estudiar la legislación europea sobre criptomonedas, por lo que no se volverán a repetir, pero sirven para afianzar que los CASPs son actores confiables en el mercado de los criptoactivos.

Entre los CASPs se contempla los denominados *wallets*. Estos son proveedores de servicios de custodia de criptomonedas, y en algunos casos también intermediarios de transacciones. En el caso de Bitcoin, se puede optar por una amplia variedad de *wallets*. Las “*wallets* custodias” ostentan la titularidad de las criptomonedas en nombre de un tercero. Las “*wallets* no custodias” solamente guardan las claves de los usuarios para que no las pierdan. Como el bitcoin es indisponible sin clave, perderla es equiparable a destruir las criptomonedas de las que se ostentase titularidad, pues estas se vuelven irre recuperables. La empresa cripto-

forense Chainalysis estimó en 2020 que alrededor del 20% de los Bitcoins minados hasta entonces se habían perdido irreversiblemente<sup>30</sup>. La custodia de criptomonedas mediante *wallets* es una práctica ampliamente extendida, por su conveniencia y seguridad. Aunque no sean completamente infalibles ante ataques de *hackers*, las *wallets* más reputadas son extremadamente confiables, y la mayoría de usuarios de criptomonedas las emplean en menor o mayor medida. Una persona puede tener cuantas *wallets* contrate, lo cual nos abre un mar de posibilidades.<sup>31</sup>

Nuestra propuesta para solventar los problemas de identificación, determinación y constitución, así como parte del problema de ejecución, es crear una “*wallet custodia*” que sirva como depósito de las criptomonedas sobre las que se quiere establecer una garantía. De esta forma, estamos haciendo que un conjunto de criptomonedas sea determinado y específico. La clave privada (CF) de este *wallet* se entregarán en un sobre cerrado a un notario o tercero de confianza, quien las guardará hasta el momento en que el crédito se satisfaga o sea necesario ejecutar las garantías. Con esto se solventan tres problemas. Primero, las criptomonedas serán indisponibles durante en término de la garantía. También se aporta protección a terceros, puesto que las criptos no podrán ser transmitidas a personas que desconozcan la garantía que las grava. Por último, en caso de impago, será posible ejecutar las criptomonedas, puesto que se tiene la clave de la *wallet*.

El depósito mediante “*wallet custodia*” nos permite constituir una prenda ordinaria, pues cumplimos los requisitos de identidad y especificación, y se da un traslado posesorio de las criptomonedas al entregar las claves a un tercero, que las tendrá en “depósito” hasta el momento de ejecución o restitución. Aunque en la práctica el *wallet* ostente la posesión de las criptomonedas, la titularidad de dicho bitcoin figurará en la Blockchain como la del deudor. Esta separación entre posesión y propiedad solo es posible porque la *wallet* es un CASP al que el titular de las criptomonedas ha confiado sus claves, pero que por el contrato que los vincula y las obligaciones como proveedor de servicios bajo el MiCA, tiene prohibido disponer de las mismas. Además, al no ser la *wallet* el acreedor de la garantía, esta no se extingue por confusión ni se corre el riesgo de incumplir el pacto comisorio. La constitución de este depósito se llevará

---

<sup>30</sup> Hayes, A. (22 diciembre 2024). *What Happens to Bitcoin After All 21 Million Are Mined?* Investopedia. <https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/>

<sup>31</sup> Ehrlich, S. (s. f.). What are crypto wallets? Forbes. <https://www.forbes.com/sites/digital-assets/article/what-are-crypto-wallets/>

a cabo en escritura pública o póliza ante fedatario público para garantizar su oponibilidad frente a terceros y su ejecutabilidad sumaria.

## 2. FIRMA DE UN PACTO MARCIANO

Otro de nuestros objetivos es agilizar la ejecución de la garantía. Para lograr esto proponemos establecer un pacto marciano, mencionado anteriormente. El pacto marciano es una nueva vía de ejecución de garantías, legitimada por la Dirección General de los Registros y del Notariado (actualmente la DGSJFP) en su resolución de 26 de diciembre 2018<sup>32</sup>. En esta se consideraba válida la configuración dada a un pacto marciano como mecanismo para llevar a cabo la venta extrajudicial de un bien dado en garantía. Su argumentación se fundamenta en que la prohibición del pacto comisorio busca evitar que el acreedor se enriquezca injustamente valorando el bien por debajo de su valor real, y asegurar el mejor precio de venta mediante el procedimiento de ejecución del bien. El pacto marciano, por su configuración, evita el enriquecimiento injusto del acreedor y asegura el mejor precio de venta del bien, puesto que incluye un procedimiento de valoración justo que salvaguarda los intereses del deudor y de terceros. La resolución se apoya en el anteriormente mencionado Real Decreto-ley 5/2005, en particular su artículo 11, como excepción legal a la prohibición del pacto comisorio, demostrando que esta prohibición no es absoluta. La STS 24 junio 2010<sup>33</sup>, y más recientemente la STS de 27 de junio 2023<sup>34</sup>, admiten como válido en nuestro ordenamiento jurídico el pacto marciano; y la STS de 21 febrero 2017<sup>35</sup>, deniega la inscripción de un pacto marciano por no prever un procedimiento de valoración lo suficientemente objetivo.<sup>36 37</sup>

---

<sup>32</sup> Resolución de 26 de diciembre de 2018, de la Dirección General de los Registros y del Notariado, en el recurso interpuesto contra la nota de calificación extendida por la registradora mercantil y de bienes muebles II de Santa Cruz de Tenerife, por la que se deniega la inscripción de determinados pactos de una hipoteca naval.

<sup>33</sup> Sentencia Tribunal Supremo, Sala de lo Civil, nº 3753/2010, de 24 de junio de 2010

<sup>34</sup> Sentencia Tribunal Supremo, Sala de lo Civil, nº 2994/2023, de 27 de junio de 2023

<sup>35</sup> Sentencia Tribunal Supremo, Sala de lo Civil, nº 581/2017, de 21 de febrero de 2017

<sup>36</sup> Ávila, G. (2019). *Validez del pacto marciano como procedimiento extrajudicial de ejecución de garantías*. Pérez Llorca Despacho de Abogados. <https://www.perezllorca.com/wp-content/uploads/2019/02/Nota-Jur%C3%ADdica-Validez-del-Pacto-Marciano-como-procedimiento-extrajudicial-de-ejecuci%C3%B3n-de-garant%C3%ADas.pdf>

<sup>37</sup> Área de Conocimiento e Innovación. (24 julio 2023). *A vueltas con el pacto comisorio*. Despacho Cuatrecasas. <https://www.cuatrecasas.com/es/spain/financiero/art/pacto-comisorio-prohibicion>

Mediante el establecimiento de un pacto marciano, en caso de impago, el acreedor solicitará las claves al tercero de confianza y podrá dirigirse directamente al mercado para vender las criptomonedas depositadas en la *wallet*, imputando el beneficio al pago de la deuda y devolviendo al deudor o a sus acreedores el remanente. Las criptomonedas se valorarán justamente porque dicha apreciación ser llevará a cabo por el mercado abierto y transparente, y no por el propio acreedor, en el momento de la venta posterior al incumplimiento. El acreedor está interesado en obtener el mejor valor por estas criptomonedas, puesto que no se las va a apropiarse y por lo tanto no obtendría ningún beneficio de venderlas por menos de su valor real.

### 3. PACTO LOMBARDO Y CLÁUSULA LTV

El último problema que debemos solucionar es el de la volatilidad de las criptos, y para ello recurriremos a una cláusula de estabilización Loan-To-Value (LTV) con la estructura de un crédito lombardo. Los créditos lombardos son una forma de préstamo ideal para mercados de alta volatilidad y gran inflación, que permite obtener financiación con flexibilidad. El colateral u objeto de garantía en estos créditos es un bien altamente volátil, como una cartera de valores o, en nuestro caso, una criptomoneda.<sup>38</sup>

Al formular un crédito lombardo, surge la necesidad de establecer un mecanismo que asegure una liquidez mínima al acreedor en caso de necesitar ejecutar la garantía, para que no se encuentre con que esta ha quedado “vacía” al desplomarse su valor durante el periodo de pago. Para ello, primero se evalúa el bien objeto de garantía, y se establece una valoración de referencia para el mismo, generalmente el valor de mercado en cada momento. También se determina un porcentaje sobre la cuantía o crédito garantizado, denominado el ratio LTV, y servirá como referencia para asegurar que la garantía pueda en todo momento cubrir el crédito garantizado. Cuanto más volátil sea el activo pignorado, mayor será el ratio LTV. Por ejemplo, un LTV para una criptomoneda puede ser del 120%. Esto significa que para garantizar un crédito de 100k, el deudor deberá depositar criptomonedas hasta un valor de 120k. Durante el periodo de garantía, si el valor del bien pignorado cayese por debajo del LTV, el deudor deberá incrementar la garantía aportando más colateral, hasta que se estabilice el LTV. En un escenario en el que el valor de bitcoin se desplomase, y el depósito pasase a valer 100k, el deudor deberá introducir más bitcoins en la *wallet* hasta que vuelva a alcanzar 120k, el ratio LTV de 120%

---

<sup>38</sup> Deutsche Bank España. (30 noviembre 2023). *Crédito Lombardos: una alternativa de liquidez*. Espacio de Finanzas, Deutsche Bank España. <https://www.deutsche-bank.es/es/blog/educacion-financiera/credito-lombardos-una-alternativa-de-liquidez.html>

establecido. Por otro lado, en los créditos lombardos se le permite al deudor cierta disposición de los bienes objeto de garantía, siempre que respete el LTV. Esta clase de préstamos llevan siendo usados por pequeños y medianos inversores en nuestro sistema jurídico, sin incidencias, desde al menos 2022, aunque son comunes en Blanca Privada desde mucho antes.<sup>39 40 41</sup>

Con estas tres características, hemos logrado constituir una prenda ordinaria sobre criptomonedas, creando desplazamiento posesorio mediante el depósito frente a tercero en una *wallet*, mediante escritura pública o póliza intervenida para que sea oponible frente a terceros. El depósito de las criptos también permitirá ejecutar las garantías en caso de necesidad. Además, para facilitar dicha ejecución hemos previsto un pacto marciano en virtud del cual el acreedor podrá dirigirse directamente al mercado para realizar los bitcoins, sin necesidad de subasta pública ni intervención judicial. Por último, para asegurar que la garantía retenga suficiente valor para poder compensar el crédito principal, hemos establecido un ratio LTV que obligará al deudor a asegurar que el valor total de las criptomonedas en la *wallet* siempre supere un determinado porcentaje sobre el principal del crédito garantizado.

#### 4. PROPUESTA DE CLÁUSULA DE GARANTÍA SOBRE CRIPTOMONEDAS

Cláusula [●]: Constitución de prenda sobre criptomonedas.

1. **Constitución.** En garantía del cumplimiento de la obligación principal (el **Crédito**), y sin perjuicio de la responsabilidad personal e ilimitada del deudor, las partes acuerdan constituir un derecho real de prenda sobre criptomonedas Bitcoin (BTC) titularidad del deudor pignoraticio. Las unidades de BTC titularidad del deudor necesarias para cubrir un 120% del principal del Crédito (la **Prenda**), han sido previamente transferidas a la “*wallet* custodia” identificada como [●], con dirección pública [●], constituida expresamente para los efectos de esta garantía (el **Depósito**).

---

<sup>39</sup> Deutsche Bank España. (30 noviembre 2023). *Crédito Lombardos: una alternativa de liquidez*. Espacio de Finanzas, Deutsche Bank España. <https://www.deutsche-bank.es/es/blog/educacion-financiera/credito-lombardos-una-alternativa-de-liquidez.html>

<sup>40</sup> Banco Santander. (3 enero 2023). *Préstamo lombardo o colateral: ¿Qué es?* Santander Consumer. <https://www.santanderconsumer.es/blog/post/prestamo-lombardo-o-colateral-que-es>

<sup>41</sup> De la Quintana, L. (9 abril 2022). *Usted ya puede pignorar su cartera para invertir un 50% más*. elEconomista.es. <https://www.eleconomista.es/mercados-cotizaciones/noticias/11711368/04/22/Usted-ya-puede-pignorar-su-cartera-para-invertir-un-50-mas.html>

2. **Desplazamiento Posesorio.** La clave privada del Depósito se entregará en sobre cerrado al tercero de confianza D/Dña [●], con Documento Nacional de Identidad [●], [Notario interviniente del presente contrato] (el **Depositario**). El Depositario se compromete a conservar la clave con la debida diligencia, absteniéndose de utilizarla bajo ningún concepto. Cuando el Crédito haya quedado satisfecho, se procederá a la cancelación de la prenda entregando el Depositario la clave privada al deudor para que recupere la disposición sobre la Prenda (los BTC).
3. **Ejecución.** En caso de impago total o parcial del Crédito a su vencimiento, habiéndose notificado formalmente al deudor dicho incumplimiento y resultando la cantidad vencida líquida y exigible, el acreedor solicitará al Depositario la entrega de la clave privada para proceder a ejecutar la Prenda. La Prenda se ejecutará mediante su venta directa en el mercado abierto en los tres días hábiles siguientes a la entrega de la clave privada, acudiendo a uno de los *exchange* acordados por las partes (Binance, Kraken, Coinbase u otro de características y reconocimiento similar), y aplicando el valor de cotización de BTC en el momento exacto de la venta, conforme al tipo de cambio BTC/EUR. El importe obtenido de esta venta se destinará primero al pago del Crédito, incluyendo intereses y costes contractuales. Una vez satisfecho el Crédito, el valor remanente, su hubiese, será devuelto al deudor en su totalidad en un plazo máximo de 5 días hábiles desde la liquidación de la Prenda. En caso de no existir remanente, la parte que permanezca impagada del Crédito subsistirá.
4. **Estabilización de la Garantía.** Durante la vigencia del Crédito, las partes acuerdan que el valor de la Prenda en ningún caso será inferior al 120% del valor del Crédito (el **Ratio LTV**). A estos efectos, se monitorizará el valor de la Prenda en Euros (€) cada semana, siguiendo el tipo de cambio BTC/EUR marcado por CoinMarketCap<sup>42</sup>. Si se da el caso de que el valor de la Prenda sea inferior al Ratio LTV, el deudor tendrá 4 días para transferir más BTC al Depósito, a contar desde la recepción de la notificación del acreedor. Estos BTC pasarán a formar parte de la Prenda, restaurando así el Ratio LTV debido. El incumplimiento de esta obligación facultará al acreedor para considerar el vencimiento anticipado de la garantía, y proceder a su ejecución conforme a lo pactado.

---

<sup>42</sup> CoinMarketCap. (s.f.) *Calculate BTC to EUR live today (BTC-EUR)*. CoinMarketCap. <https://coinmarketcap.com/currencies/bitcoin/btc/eur/>

## **VI. CONCLUSIONES Y PROPUESTAS**

Concluimos con la cláusula de prenda sobre criptomonedas este trabajo de fin de grado. La realidad de las criptos se vuelve más relevante cada día, y con ella la necesidad de entenderlas y darles una regulación apropiada. En este trabajo se ha intentado arañar la superficie de dicha cuestión, teniendo en cuenta que muchas de las problemáticas jurídicas y prácticas planteadas podrían ser objeto de su propia investigación. Aún así, los resultados han sido satisfactorios, y hemos conseguido combinar la naturaleza técnica y descentralizada de las criptomonedas con los principios del sistema de garantías reales español. Pese a los obstáculos, es posible construir soluciones jurídicas viables para las nuevas realidades de Fintech.

Al revisar los objetivos con los que enfoqué este trabajo, estoy satisfecha con los resultados. Las primeras dos secciones me han permitido comprender el funcionamiento más básico de las criptomonedas. He podido poner a prueba mis conocimientos con amigos interesados en el tema y he comprobado que efectivamente entiendo los principios generales del Bitcoin, y que esta comprensión básica me ha abierto las puertas a una visión de la tecnología y las finanzas que antes no tenía. En cuanto al régimen legislativo de las criptomonedas, ha sido muy interesante entrar a investigar una materia tan joven, pues se pueden detectar las intenciones de los legisladores y observar cómo estas leyes impactan a la realidad en tiempo real. Creo que el Reglamento MiCA es un buen punto de partida para legislar el Fintech, pero regulaciones más concretas son necesarias para extender el uso de estos activos y proteger a inversores pequeños y medianos. Por supuesto, hacer esto está reñido con permitir que las tecnologías continúen su desarrollo, razón por la que soluciones como la propuesta en este trabajo son tan importantes para dar encaje a los criptoactivos en nuestro sistema.

En cuanto al segundo objetivo, considero que mis conocimientos sobre garantías se han desarrollado significativamente. Para el estudio del tema, elegí dos obras doctrinales con rasgos diferentes: el libro de Díez-Picazo buscaba el análisis de un reconocido jurista, mientras que el de Verda y Beamonte suplía una visión más actualizada y transversal del asunto. Haber podido profundizar en los diferentes tipos de garantías me ha dado una visión mucho más minuciosa del abanico de opciones que ofrece nuestro ordenamiento jurídico para adaptarse a todas las realidades posibles. Ha sido particularmente complejo el análisis de la naturaleza jurídica de las criptomonedas, debido a la abundancia de puntos de vista disidentes que existen. Finalmente

opté por las interpretaciones que me parecían más coherentes con lo que había aprendido sobre estos criptoactivos, y que encajaba mejor con el objetivo de este trabajo.

Aplicar los conocimientos adquiridos en la investigación para identificar la problemática de las criptomonedas a la hora de ser objeto de garantía ha sido la parte más desafiante del trabajo. Ha requerido muchas lecturas y conversaciones para hallar soluciones coherentes y elegantes a los problemas que iban surgiendo, examinando mecanismos legales que conocía solo periféricamente como el pacto marciano o el crédito lombardo. Al final ha sido la parte más gratificante de este estudio, pues me ha permitido demostrar que he asimilado los conocimientos adquiridos y he desarrollado una lógica jurídica durante la carrera que me ha permitido enfrentar este problema. Haber podido adaptar una figura jurídica que percibía como algo “estática” (la prenda) a una realidad de rabiosa actualidad con una naturaleza etérea y descentralizada me abre los ojos a las posibilidades que el derecho ofrece y las cuestiones que aún le quedan por conquistar.

Me ha faltado espacio para poder explorar otras alternativas de garantía que se me han ocurrido. Una de ellas era la posibilidad de configurar el depósito y la ejecución automática de la garantía mediante un Smart Contract, permitiendo que una nueva tecnología dé solución a otra. También me interesaba la posibilidad de instaurar un registro oficial internacional donde poder inscribir gravámenes sobre criptoactivos. Además, en un momento dado planteé la opción de instar una reforma de la LHMPD para incluir las criptomonedas, en base al razonamiento jurídico de Reig Palmero sobre el criterio de clasificación de los objetos de las prendas sin desplazamiento. En cualquier caso, no dejo de subrayar la importancia de delimitar con oficialidad la naturaleza jurídica de estos instrumentos para poder facilitar su integración en nuestro sistema.

También se me queda en el tintero una exploración de otras iniciativas globales que empiezan a jugar con las criptomonedas como herramientas financieras. Desde el Observatorio Blockchain destacan varios proyectos, como el liderado por el BBVA en Suiza, que desde junio de 2021 ofrece a sus clientes servicios similares a los de los CASPs; o el de Deutsche Bank, que ofrece servicios de custodia de criptoactivos<sup>43</sup>. La plataforma on-line Nebeus ofrece préstamos

---

<sup>43</sup> Maldonado, J. (16 noviembre 2023). *Los bancos más importantes del mundo ya ofrecen bitcoin y criptomonedas*. Observatorio Blockchain. <https://observatorioblockchain.com/criptomonedas/los-bancos-mas-importantes-del-mundo-ya-ofrecen-bitcoin-y-criptomonedas>

respaldados por criptomonedas como garantía<sup>44</sup>. También se han dado avances legislativos fuera de la Unión Europea. Nueva York desarrolló en 2015 un marco normativo para CASPs que sigue activo, coloquialmente denominado BitLicense, para “garantizar que los neoyorquinos dispongan de una forma bien regulada de acceder al mercado de las criptomonedas y que Nueva York siga estando en el centro de la innovación tecnológica y la regulación con visión de futuro.”<sup>45</sup> Alemania ha dado el paso de calificar jurídicamente a las criptomonedas: la Autoridad Federal de Supervisión Financiera las ha denominado instrumentos financieros, sujetos a su autoridad. Esta calificación apoya nuestro argumento de que pueden establecerse garantías sobre bitcoin<sup>46</sup>. Es probable que en los próximos años veamos aún más movimiento en este ámbito, según el mercado se adapte al MiCA, los bitcoins minados lleguen a su límite máximo de 21 millones (estamos entorno a los 19 millones), y el nuevo presidente de Estados Unidos Donald Trump ponga en marcha la promesa electoral que denominó “Crypto Project”.

Antes de terminar, es pertinente advertir de los riesgos de las criptomonedas, pues esta nueva tecnología, a pesar de todas sus posibilidades, también plantea problemas de los que es conveniente ser consciente. Su aceptación a gran escala cambiaría el sistema bancario y financiero como los conocemos, minando la autoridad de los intermediarios y las figuras reguladoras del mercado. A nivel gubernamental y regulativo existe la misma amenaza, pues no debemos olvidar que el bitcoin y el blockchain son ideas surgidas de grupos con tendencias cyberanarquistas. La falta de supervisión en estas herramientas facilita la evasión fiscal y la financiación de actividades ilegales, incluso con la normativa AMLD5. Se trata de una tecnología difícil de comprender, lo cual también expone a los consumidores a fraudes y estafas, ejemplos de los cuales ya hemos visto, así como a quedar expuestos a grandes pérdidas por su alta volatilidad. Y por supuesto, falta hablar del impacto ambiental de esta tecnología. El elevado Poder CPU requerido para general el proof-of-work y minar bitcoin consume

---

<sup>44</sup> Nebeus. (s. f.). *Préstamos respaldados por Bitcoin y otras criptomonedas*. <https://nebeus.com/es/loans>

<sup>45</sup> NY Department Of Financial Services. (s.f.). Virtual currency business licensing. [https://www.dfs.ny.gov/virtual\\_currency\\_businesses](https://www.dfs.ny.gov/virtual_currency_businesses) [traducción realizada por la alumna]

<sup>46</sup> Sala de Redacción de CriptoNoticias. (4 marzo 2020). *Autoridad supervisora alemana declara a las criptomonedas como instrumentos financieros*. CriptoNoticias. <https://www.criptonoticias.com/regulacion/autoridad-supervisora-alemana-criptomonedas-instrumentos-financieros/>

cantidades ingentes de energía, que llevan a muchos expertos a advertir del impacto climático del Fintech.

De ahora en adelante, las criptomonedas desempeñarán un papel creciente en los mercados internacionales. Una regulación adecuada es clave para poder sacarles todo el provecho posible como herramientas del tráfico jurídico. La inclusión de estas herramientas en nuestro ordenamiento es necesaria para proteger a los actores a todos los niveles y mantenernos al frente de la innovación, respetando la vocación del Derecho de supervisar y proteger los valores fundamentales del nuestro Ordenamiento Jurídico.

## VII. BIBLIOGRAFÍA

### A. Legislación

Decreto, de 8 de febrero de 1946, por el que se aprueba la nueva redacción oficial de la Ley Hipotecaria.

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.

Ley, 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Ley, de 16 de diciembre de 1954, sobre hipoteca mobiliaria y prenda sin desplazamiento de posesión

Real Decreto, de 24 de julio de 1889, por el que se publica el Código Civil.

Real Decreto-ley 5/2005, de 11 de marzo, de reformas urgentes para el impulso a la productividad y para la mejora de la contratación pública

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.

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

Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

### B. Jurisprudencia

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)*. <https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf>

Banco de España. (10 julio 2024). *Aplicación del Reglamento relativo a los mercados de criptoactivos (MiCAR) respecto de la emisión de ART y EMT*. Banco de España. <https://www.bde.es/f/webbe/GAP/Secciones/SalaPrensa/NotasInformativas/24/presbe2024-58.pdf>

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.

CNMV. (s.f.). *MiCA: Nueva regulación de criptoactivos*. CNMV. <https://www.cnmv.es/portal/mica/regulacion-criptoactivos.aspx?lang=es>

Resolución de 26 de diciembre de 2018, de la Dirección General de los Registros y del Notariado, en el recurso interpuesto contra la nota de calificación extendida por la registradora mercantil y de bienes muebles II de Santa Cruz de Tenerife, por la que se deniega la inscripción de determinados pactos de una hipoteca naval.

Resolución Vinculante de Dirección General de Tributos, V1149-18, de 08 de mayo de 2018

Sentencia Tribunal de Justicia de la Unión Europea. Asunto C-264/14 (Skatteverket / David Hedqvist) de 22 de octubre de 2015

Sentencia Tribunal Supremo, Sala de lo Civil, nº 2994/2023, de 27 de junio de 2023.

Sentencia Tribunal Supremo, Sala de lo Civil, nº 3753/2010, de 24 de junio de 2010.

Sentencia Tribunal Supremo, Sala de lo Civil, nº 581/2017, de 21 de febrero de 2017

Sentencia Tribunal Supremo, Sala de lo Penal, nº326/2019, de 20 de junio de 2019

### C. Obras doctrinales

Área de Conocimiento e Innovación Cuatrecasas. (24 julio 2023). *A vueltas con el pacto comisorio*. Despacho Cuatrecasas.

<https://www.cuatrecasas.com/es/spain/financiero/art/pacto-comisorio-prohibicion>

- Asensio Borrellas, V. (5 julio 2019). *El bitcoin: una primera aproximación jurídica en derecho civil español*. Lefebvre: El Derecho. <https://elderecho.com/bitcoin-una-primer-a-proximacion-juridica-derecho-civil-espanol>
- Ávila, G. (2019). *Validez del pacto marciano como procedimiento extrajudicial de ejecución de garantías*. Pérez Llorca Despacho de Abogados. <https://www.perezllorca.com/wp-content/uploads/2019/02/Nota-Jur%20dica-Validez-del-Pacto-Marciano-como-procedimiento-extrajudicial-de-ejecuci%20n-de-garant%20Das.pdf>
- Boehm, F y Pesch, P. (2014). *Bitcoin: A First Legal Analysis - with reference to German and US-American law*. University of Münster. <https://www.zar.kit.edu/downloads/Publikationen/Franziska%20Boehm/BTC%20final%20camready.pdf>
- 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. <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/>
- Díez-Picazo, L. (2012). *Los derechos reales de garantía. El derecho real de prenda. El derecho real de hipoteca. La hipoteca mobiliaria (I). La hipoteca mobiliaria (II). La prenda sin desplazamiento de posesión*. En Díez-Picazo, L. (2012). *Fundamentos del derecho civil patrimonial VI: derechos reales* (1ª ed.). Editorial Civitas.
- Fonticiella Hernández, B. (2021). *La protección del inversor minorista en el panorama Fintech. Crowdfunding. Criptomonedas. Initial Coin Offerings. (ICO)*. Editorial Dickinson.
- Girgado Perandones, P. (2023). *La prenda mercantil*. En Ramón de Verda y Beamonte, et al (Coord.). *Derechos Reales (Tratado práctico interdisciplinar)* (1ª ed.). Editorial Tirant Lo Blanch.
- Reig Palmero G. (2023). *La hipoteca mobiliaria y la prenda sin desplazamiento*. En Ramón de Verda y Beamonte, et al (Coord.). *Derechos Reales (Tratado práctico interdisciplinar)* (1ª ed.). Editorial Tirant Lo Blanch.

Ruiz Rodríguez, R. (2020). *Las criptodivisas como medio de pago y el Derecho internacional privado*. CUADERNOS DE DERECHO TRANSNACIONAL, 12(2), 740-757.  
<https://doi.org/10.20318/cdt.2020.5628>

Sedeño López, J.F. (2020). *Naturaleza jurídica de las criptomonedas. Análisis de la STS de 20 de junio de 2019, rec. núm. 998/2018*. Revista de Contabilidad y Tributación. CEF, 442 (enero 2020), pp. 116-121.

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.  
[https://www.uria.com/documentos/circulares/1417/documento/12353/Nota\\_clientes.pdf?id=12353](https://www.uria.com/documentos/circulares/1417/documento/12353/Nota_clientes.pdf?id=12353)

Verda y Beamonte, J.R. (2023) *Los derechos reales de garantía: la prenda*. En Ramón de Verda y Beamonte, et al (Coord.). *Derechos Reales (Tratado práctico interdisciplinar)* (1ª ed.). Editorial Tirant Lo Blanch.

#### D. Recursos de internet

Amelia. (s.f.). *10 Biggest Falls in Bitcoin History: Bitcoin's Biggest Crashes*. The Network Journal. <https://tnj.com/biggest-falls-in-bitcoin-history/>

Ashford, K. (21 mayo 2024). *What is bitcoin and how does it work?*. Forbes Advisor. <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-bitcoin/>

Banco Santander. (3 enero 2023). *Préstamo lombardo o colateral: ¿Qué es?* Santander Consumer. <https://www.santanderconsumer.es/blog/post/prestamo-lombardo-o-colateral-que-es>

BBVA. (20 abril 2023). *Regulación europea sobre mercados de criptoactivos (MiCA): qué es y por qué es importante*. Comunicaciones BBVA. <https://www.bbva.com/es/innovacion/regulacion-europea-sobre-mercados-de-criptoactivos-mica-que-es-y-por-que-es-importante/>

Bitcoin (s.f.) *Development*. Bitcoin. <https://bitcoin.org/en/development#bitcoin-core-contributors>

- Bitcoin. (s.f.). *The Bitcoin Revolution: How It All Started and Where We Are Now*. Bitcoin.com. <https://www.bitcoin.com/get-started/the-bitcoin-revolution/#:~:text=Explore%20the%20origins%20of%20Bitcoin%2C%20its%20impact%20on,regulatory%20landscape%2C%20and%20the%20future%20of%20digital%20currencies>
- CoinGlass. (s. f.). *Bitcoin historical volatility*. Coinglass. <https://www.coinglass.com/es/pro/i/bl>
- De la Quintana, L. (9 abril 2022). *Usted ya puede pignorar su cartera para invertir un 50% más*. elEconomista.es. <https://www.eleconomista.es/mercados-cotizaciones/noticias/11711368/04/22/Usted-ya-puede-pignorar-su-cartera-para-invertir-un-50-mas.html>
- Deutsche Bank España. (30 noviembre 2023). *Crédito Lombardos: una alternativa de liquidez*. Espacio de Finanzas, Deutsche Bank España. <https://www.deutsche-bank.es/es/blog/educacion-financiera/credito-lombardos-una-alternativa-de-liquidez.html>
- Ehrlich, S. (s. f.). *What are crypto wallets?* Forbes. <https://www.forbes.com/sites/digital-assets/article/what-are-crypto-wallets/>
- Hayes, A. (22 diciembre 2024). *What Happens to Bitcoin After All 21 Million Are Mined?* Investopedia. <https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/>
- Jiménez Sanchez-Mora, J. (22 abril 2021). *Caso Arbistar: la mayor estafa piramidal con criptomonedas*. Economist&Jurist. <https://www.economistjurist.es/economia/caso-arbistar-la-mayor-estafa-piramidal-con-criptomonedas/>
- Macheel, T. (29 noviembre 2024). *Bitcoin heads for nearly 40% November gain as it edges closer to \$100,000*. CNBC. <https://www.cnbc.com/2024/11/29/bitcoin-heads-for-nearly-40percent-november-gain-as-it-edges-closer-toward-100000.html?msockid=13e44d9df04967351bd95e10f18a6655>

- Maldonado, J. (16 noviembre 2023). *Los bancos más importantes del mundo ya ofrecen bitcoin y criptomonedas.* Observatorio Blockchain. <https://observatorioblockchain.com/criptomonedas/los-bancos-mas-importantes-del-mundo-ya-ofrecen-bitcoin-y-criptomonedas>
- Nakamoto, S. (2008) *Bitcoin: A peer-to-peer Electronic Cash System.* Editorial Bitcoin, UK. <https://bitcoin.org/bitcoin.pdf>
- Nebeus. (s. f.). *Préstamos respaldados por Bitcoin y otras criptomonedas.* <https://nebeus.com/es/loans>
- NY Department Of Financial Services. (s.f.). *Virtual currency business licensing.* [https://www.dfs.ny.gov/virtual\\_currency\\_businesses](https://www.dfs.ny.gov/virtual_currency_businesses)
- Rasure, E. (24 de enero de 2025). *What Was the Silk Road Online? History and Closure by the FBI.* Investopedia. <https://www.investopedia.com/terms/s/silk-road.asp>
- Rothrie, S. (22 mayo 2020). *Who Controls Bitcoin? A Guide to BTC Stakeholders.* Crypto Briefing. <https://cryptobriefing.com/who-controls-bitcoin-guide-btc-stakeholders/>
- Sala de Redacción de CriptoNoticias. (4 marzo 2020). *Autoridad supervisora alemana declara a las criptomonedas como instrumentos financieros.* CriptoNoticias. <https://www.cryptonoticias.com/regulacion/autoridad-supervisora-alemana-criptomonedas-instrumentos-financieros/>

## ANEXO I – Definiciones

<b>AMLD5</b>	Directiva (UE) 2018/843 (AMLD5), sobre la prevención del blanqueo de capitales y la financiación del terrorismo
<b>Blockchain</b>	Herramienta de Fintech empleada para minar criptomonedas
<b>CASPs</b>	<i>Cripto-Assets Service Providers</i> o Proveedores de servicios relacionados con criptoactivos, por sus siglas en inglés.
<b>CF</b>	Clave de Firma o Firma Privada
<b>CHF</b>	Funciones Criptográficas Hash
<b>Criptomonedas, criptos o Bitcoin</b>	Empleados indistintamente para referirse a la moneda Bitcoin (BTC).
<b>CV</b>	Clave de Verificación o Firma Pública
<b>Double Spending</b>	El problema del doble gasto de criptomonedas, que Nakamoto consigue resolver al crear Bitcoin
<b>Fintech</b>	Abreviatura de <i>Financial Technology</i> , empleado para referirse a las innovaciones financieras derivadas de las nuevas tecnologías.
<b>LHMPSD</b>	Ley, de 16 de diciembre de 1954, sobre hipoteca mobiliaria y prenda sin desplazamiento de posesión
<b>MiCA</b>	Reglamento Europeo sobre Mercados de Criptoactivos
<b>Nodos</b>	Usuarios de cualquier red de intercambio de criptomonedas, encargados de verificar la correspondiente Blockchain
<b>Poder CPU</b>	Esfuerzo computacional necesario para generar <i>proof-of-work</i>
<b>Proof-of-work</b>	Herramienta empleada para proteger la Blockchain de nodos malignos
<b>Wallets</b>	Del inglés <i>carteras</i> , así se denominan los servicios de custodia de criptomonedas.