



Universidad
Zaragoza

Trabajo Fin de Grado

ASPECTOS JURÍDICOS DE LA TECNOLOGÍA BLOCKCHAIN

Autor

Eduardo Carceller Ortega

Director

Javier Usoz Otal

Facultad de Derecho. Universidad de Zaragoza

Junio de 2022

INDICE

1. INTRODUCCIÓN.....	1
1.1. MOTIVACIÓN DEL TRABAJO	1
1.2. APROXIMACIÓN AL CONCEPTO DE TENOLOGÍA BLOCKCHAIN:	1
A. CARACTERÍSTICAS	4
B. TIPOS DE BLOCKCHAIN:	7
2. ASPECTOS JURÍDICOS DE LA TECNOLOGÍA BLOCKCHAIN:	8
2.1. IMPLICACIONES JURÍDICAS DE LAS APLICACIONES DE LA TECNOLOGÍA BLOCKCHAIN:	9
A. CRIPTOACTIVOS:	10
a) ¿Qué son?	10
b) Normativa y retos jurídicos:	13
B. SMART CONTRACTS:	25
a) ¿Qué son?.....	25
b) Normativa y retos jurídicos:	27
2.2. IMPLICACIONES JURÍDICAS DE LAS CARACTERÍSTICAS DE LA TECNOLOGÍA BLOCKCHAIN:	30
A. Protección de datos personales: derecho al olvido	30
a) Problema	31
b) Solución.....	32
3. CONCLUSIONES	33
4. BIBLIOGRAFÍA	37

1. INTRODUCCIÓN

1.1. MOTIVACIÓN DEL TRABAJO

Hoy en día existen pocos ámbitos en los que todavía no ha entrado la regulación. En un mundo en el que para casi cualquier situación de la vida existe una norma a la que acudir cuando surge algún conflicto, se hace difícil pensar en que haya alguna de esas situaciones en las que, si surge algún problema, no se cuente con mecanismos de resolución de conflictos.

La tecnología blockchain y sus numerosas aplicaciones son un ejemplo de esas pocas situaciones que se encuentran en la actualidad «huérfanas» de regulación. A raíz de esta tecnología han surgido numerosas aplicaciones que han dado lugar a nuevas formas de compartir información y valor o a nuevos productos o servicios, como los criptoactivos, las cuales han formado un mercado secundario de compra y venta de los mismos que ha llegado a tener una capitalización de casi 3 billones de dólares a nivel mundial¹ y en el que invierten más del 15% de españoles².

Con datos tan relevantes, la regulación en el ámbito de la tecnología blockchain es inevitable y los ordenamientos jurídicos ya está buscando fórmulas para la creación de un marco normativo para las nuevas figuras surgidas a partir de la misma acorde a los riesgos que conllevan pero teniendo en cuenta el no interrumpir en demasía el proceso de innovación tecnológica que tantos beneficios puede traer.

La idea de este trabajo es hacer mención de los principales aspectos de la tecnología susceptibles de generar consecuencias jurídicas, con cierto énfasis en aquellos que tengan contenido económico, para hacer un análisis de la regulación actual que puede ser de aplicación a dichos aspectos y los retos jurídicos a los que se enfrentan los diversos ordenamientos jurídicos.

1.2. APROXIMACIÓN AL CONCEPTO DE TENOLOGÍA BLOCKCHAIN:

En primer lugar, se hace necesario describir lo que es y lo que permite la tecnología blockchain. Para entenderlo fácilmente hay que hacer referencia a dos conceptos.

¹ Capitalización total del mercado de las criptomonedas. Disponible en TradingView, <https://es.tradingview.com/chart/Njjs7Wrv/?symbol=BITSTAMP%3ABTCUSD> (Consultado 16 mayo 2022).

² MENA ROA, MÓNICA, «La adopción de las criptomonedas en el mundo», de 15 de febrero de 2022 en Statista. Disponible en: <https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/> (Consultado 16 de mayo 2022)

Por un lado, al de tecnología, la cual es la combinación de conocimientos tanto científicos como técnicos que permiten al ser humano resolver un problema³.

Por otro lado, al de blockchain, la cual es una especie de libro mayor de transacciones público que puede ejercer como un tipo específico de una base de datos no relacional⁴ en la que la información se almacena en grupos o bloques enlazados entre sí en una línea temporal. Utiliza una tecnología de registro distribuido, por ello, toda su información está distribuida por millones de ordenadores alrededor de todo el mundo. A cada ordenador se le llama nodo y serán los nodos participantes de la red blockchain en cuestión los encargados de la llevanza de estos libros mayores de transacciones⁵. De esta manera, se le otorga un carácter descentralizado a la custodia de la información contenida en las redes blockchain, pues no existe ninguna autoridad central dueña de los datos, autoridad que si existe en las bases de datos tradicionales. Además, como se explicará a continuación, debido a que los bloques se encuentran enlazados en una línea temporal, la información contenida en ellos es inmutable.

La diferencia de las redes blockchain con las bases de datos tradicionales es la inmutabilidad y la descentralización. Estas últimas son una colección de información que se almacena electrónicamente, generalmente en formato de tabla (filas y columnas), en un sistema informático en las que la modificación de un dato en la tabla puede alterar el resto de la información (modelo relacional) y, además, dichas bases de datos suelen estar en manos de un reducido grupo de personas o de una autoridad central (centralizadas), con todo lo que eso conlleva a la seguridad e integridad de los datos.

Mientras que en las bases de datos tipo blockchain, la información fluye y se acumula en una especie de libro mayor público en el que no es posible la modificación de ningún dato y no es necesaria la intervención de un tercero de confianza para verificar la veracidad de las transacciones, pues dicha verificación la llevan a cabo los participantes de la red mediante un consenso de la mayoría de los mismos.

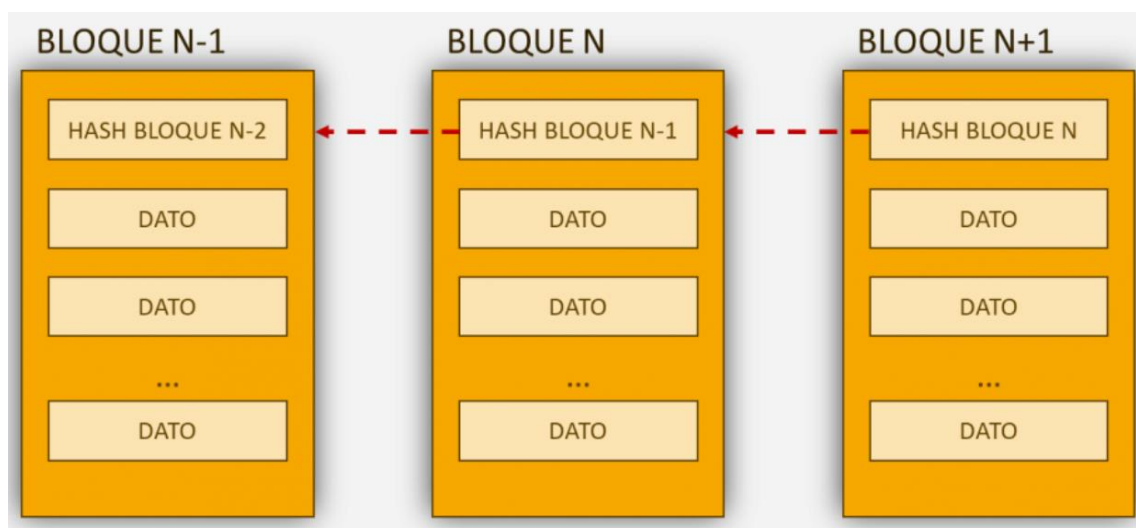
Por lo tanto, en resumidas cuentas, la tecnología blockchain es esa aplicación coordinada de conocimientos y habilidades que permite satisfacer unas necesidades del ser humano contemporáneo como son la inmutabilidad, la seguridad, la transparencia y la descentralización de la información.

³ Definición de tecnología por la RAE. Disponible en: <https://dle.rae.es/tecnolog%C3%ADa?m=form> (Consultado 25 de marzo de 2022)

⁴ Microsoft: Datos no relacionales y NoSQL. Disponible en: <https://docs.microsoft.com/es-es/azure/architecture/data-guide/big-data/non-relational-data> (Consulta: 20 de marzo 2022)

⁵ PORXAS, N. y CONEJERO, M., “Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados” *Actualidad Jurídica Uría Menéndez* n°48 año 2018 p 25.

Desde un punto de vista técnico, el funcionamiento de una red que utiliza tecnologías de registro distribuido es el siguiente. Todo empieza con un conjunto de datos, estos datos son flujos de información que se agrupan en lo que se denominan bloques, esos flujos de información se encuentran encriptados a través de criptografía y solo el receptor de la información podrá decodificar el mensaje (es por ello que se denomina red P2P: persona a persona). Para verificar que esas transacciones de datos son correctas, existe una red de ordenadores denominados nodos, distribuidos por todo el mundo, que se encargan, a partir de fuerza computacional y de técnicas criptográficas, de controlar si esas transacciones son correctas o no. Al tener todos los nodos una copia exacta de la base de datos original, si al nodo que le toca verificarlo falla, el resto de la red de ordenadores se darán cuenta del error y no darán su visto bueno (tiene que dar el visto bueno la mayoría de nodos participantes). De esta manera el bloque no será validado y no llegará a formar parte de la cadena. Si es validado correctamente, el bloque se introduce en la cadena. A través de lo que se conoce como función hash, el bloque se vuelve a encriptar con información del bloque predecesor y así, sucesivamente. De esta manera, los bloques pasan a ser inmutables, gracias a que contienen funciones hash de todos los bloques anteriores de la cadena, de forma que si se intenta modificar un bloque, se tienen que modificar absolutamente todos bloques predecesores de la cadena y tienen que dar su visto bueno al sabotaje más de la mitad de todos los nodos del planeta, lo cual es prácticamente imposible.



Fuente: Agencia Española de Protección de Datos

Esta tecnología nace con la publicación del algoritmo de Bitcoin en 2008, el cual se programó para facilitar transacciones monetarias de persona a persona sin tener que

necesitar de intermediarios. Básicamente lo que el algoritmo propone es la creación de un sistema de pagos basado en criptografía en vez de en confianza⁶. Bitcoin se convirtió así en la primera red blockchain, pero blockchain no es solo Bitcoin. En la actualidad existen numerosas redes blockchain con multitudes de utilidades diferentes. Bitcoin se creó para albergar un sistema de pagos electrónicos persona a persona sin intervención de intermediarios, pero hoy existen redes blockchain capaces de mucho más. Por ejemplo, la red blockchain de Ethereum a parte de servir como sistema de pagos descentralizado, al igual que Bitcoin, también permite crear criptoactivos en su red para transferirlos a través de la misma o alojar en ella los famosos contratos inteligentes a partir de los cuales, entre otras muchas utilidades, se pueden crear aplicaciones descentralizadas, esto es, aplicaciones en las que los usuarios interactúen en la prestación de bienes y servicios entre ellos sin ninguna autoridad central de por medio. Un ejemplo de la utilidad que tienen estas aplicaciones descentralizadas, son las llamadas finanzas descentralizadas. A partir de una aplicación descentralizada que sirva de plataforma para las personas, se pueden crear numerosos servicios financieros entre usuarios sin intervención de autoridad central alguna.

Un ejemplo de esto último son las plataformas de préstamos descentralizados, en ellas, las personas con superávit de fondos depositan fondos en dicha aplicación descentralizada y las personas con déficit de fondos cogen prestados los fondos que necesiten aportando algún activo colateral a modo de aval. De esta manera, el depositante de fondos recibirá él mismo los intereses que se generen por la utilización de sus fondos lo cual se diferencia de un depósito bancario tradicional, en los cuales, son el banco (el intermediario) el que se aprovecha de los intereses generados de unos fondos titularidad de un tercero.

A. Características

- Descentralización:

La descentralización implica que los datos de la cadena de bloques no están almacenados en un solo servidor, sino que existe una copia de toda la base de datos en cada nodo de la red y todos tienen el mismo derecho a validar transacciones y ser recompensado por ello, lo cual elimina la potencial influencia que puede tener una

⁶ Libro blanco de Bitcoin. Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf (Consultado el 12 de abril de 2022)

empresa o institución con el control de toda la información. Ningún participante de la red tiene más poder que otro por lo que se genera un sistema de intercambio de información con ausencia de intermediarios.

- **Inmutabilidad:**

Es la característica de la blockchain que hace que la información que contiene en los bloques no pueda modificarse, ya que se coteja con las copias de otros nodos, por lo que la red detectaría esa copia fraudulenta. En una blockchain, cada nodo tiene un registro completo de los datos que se han ido almacenando en la red desde su creación.

Gracias a la inmutabilidad, ningún dato que ha sido introducido en la cadena puede eliminarse ni modificarse, lo cual crea prueba irrefutable de que esa transacción del dato se ha producido en un momento del tiempo determinado.

- **Transparencia:**

Al estar distribuida por nodos alrededor de todo el mundo, las redes blockchain públicas permiten ver todas las transacciones que se realizan en la red a todos los nodos participantes e incluso, algunas como Bitcoin y Ethereum también lo permiten a los que no son nodos participantes gracias a exploradores web de sus blockchain. Cada nodo tiene su propia copia que se actualiza a medida que se confirman y añaden nuevos bloques. Esto implica que se puede seguir el rastro de una transacción que haya tenido lugar en la red en cualquier momento, lo cual se denomina trazabilidad.

Sin embargo en las redes blockchain privadas la transparencia no se da, ya que la información solo está en los ordenadores de los participantes de la red.

- **Seguridad:**

Debido a esas características de inmutabilidad y descentralización, la blockchain se convierte en una tecnología segura, ya que la información no se puede modificar para el beneficio de individuos o grupos, y no está controlada por una empresa o autoridad central, sino que la información está distribuida entre todos los nodos de la red.

Los nuevos bloques se almacenan siempre de forma lineal y cronológica: siempre se añaden al final de la cadena. Después de que un bloque se haya añadido al final de la cadena, es muy difícil volver atrás y alterar el contenido del bloque, a menos que la mayoría de nodos llegue a un consenso para poder hacerlo. Esto se debe a que cada bloque tiene su propio hash o código del bloque y una marca de tiempo. Si la información se edita de alguna manera, el código hash también cambia, por lo tanto, no encajaría con el bloque anterior⁷.

En definitiva, blockchain facilita el proceso de registro de transacciones y seguimiento de las mismas de forma transparente. En blockchain se pueden registrar transacciones de cualquier activo, bien físico, bien material. Actualmente la información es la materia prima más preciada para cualquier empresa o negocio, por ello, contra más confiable, transparente, inmediata y fácil de rastrear y consultar sea ésta, más preferible será la misma para las empresas⁸. Todas esas cualidades mencionadas se las puede aportar el registro de dicha información en una red blockchain, de ahí que se haya convertido en una tecnología disruptiva tanto para negocios existentes como para la generación de nuevos modelos de negocio.

Algunos de los usos que actualmente se le está dando a blockchain son para la mejora de la gestión de las cadenas de suministros mediante la eliminación de intermediarios. La trazabilidad y transparencia de sus registros permiten conocer en tiempo real la situación o el origen de los productos que se suministran, lo cual aporta rapidez, eficiencia y seguridad en torno a la veracidad de estas informaciones, algo útil también no solo para la eliminación de intermediarios, sino para que los consumidores conozcan con exactitud cuál es la procedencia exacta de los productos que consumen. Wal-Mart, Unilever o Nestlé son ejemplos de algunas de las compañías que han implementado esta tecnología en sus cadenas de suministro⁹.

Otros de los usos actuales y potenciales se encuentran en materia de seguros, en el ámbito de los procesos de selección de personal para el sector público, en el ámbito de la sanidad para facilitar la trazabilidad de los historiales médicos de los pacientes o,

⁷ FETSYAK, I. “Contratos inteligentes: análisis jurídico desde el marco legal español”, REDUR 18, diciembre 2020, págs. 201-202.

⁸ IBM: Visión General de Blockchain. Disponible en: <https://www.ibm.com/es-es/topics/what-is-blockchain> (Consulta: 16 de abril 2022)

⁹ BBVA Openmind: Tecnología Blockchain y gestión de la cadena de suministro. Disponible en: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/tecnologia-blockchain-y-gestion-de-cadena-de-suministro/> (Consulta: 10 de mayo 2022)

incluso, en el ámbito electoral aprovechando la transparencia, objetividad e igualdad de los votos que se puede conseguir con el uso de esta tecnología.

Sin embargo, el uso más conocido de las redes blockchain es el de las transferencias de criptoactivos, entre ellos, las criptomonedas, las cuales surgen de los incentivos que obtienen los nodos por validar transacciones de datos. Esto es debido a que, como una forma de evitar el fraude, para validar transacciones en una red blockchain pública, hay dos tipos de protocolo de consenso. Uno es el llamado Proof of Work (prueba de trabajo), en el cual se requiere de potencia computacional (llamada CPU), ya que es necesario resolver problemas criptográficos para ser elegido nodo validador¹⁰, por lo que para que salga rentable a los llamados validadores o “mineros” (nodos encargados de validar transacciones) ese gasto de energía¹¹ para la validación, se otorgan criptomonedas a estos como incentivos por mantener segura la red. Otro es el llamado Proof of Stake (prueba de participación) en el que para ser elegido nodo validador hay que bloquear criptoactivos en un contrato inteligente, teniendo más probabilidad de ser escogido nodo validador contra más criptoactivos se tengan bloqueados.

Para cada red blockchain, hay una criptomoneda nativa (para la blockchain de Bitcoin, su criptomoneda nativa es el Bitcoin; para la blockchain de Ethereum, su criptomoneda nativa es el Ether).

A parte de las criptomonedas, existen otro tipo de criptoactivos. Son los llamados *tokens*, los cuales son una especie de fichas criptográficas que representan unidades de valor. Las empresas construyen esos tokens sobre las redes blockchain capacitadas para ello (como Ethereum) y de esta manera representar cualquier clase de activo o derecho de forma digital, con el fin de ofrecérselos al público para que puedan acceder a determinados bienes o servicios, a determinados derechos o a obtener determinados incentivos entre otras utilidades. De esta manera, las empresas ofrecen al público productos en formato digital aprovechándose de las características de la tecnología blockchain (rapidez, seguridad, inmutabilidad...).

B. Tipos de blockchain:

- **Blockchain Pública:**

¹⁰ PORXAS, N. y CONEJERO, M., “Tecnología blockchain... *cit.*”, p. 28

¹¹ Se requieren unos 40kWh semanales para que compense el minado de bitcoin, según Endesa. Disponible en: <https://www.endesa.com/es/blog/blog-de-endesa/luz/cuanta-electricidad-gasta-minar-bitcoins> (Consulta: 10 mayo 2022)

Son las únicas que cuentan con todas las características descritas. En estas, no se requieren permisos para participar en la red como nodo validador, de manera que cualquiera, con los equipos necesarios puede participar.

- **Blockchain Privada:**

La participación como nodo validador en este tipo de redes requiere del permiso de los creadores de la misma. Son las más utilizadas a nivel empresarial. A pesar de perder la característica de la descentralización y la transparencia pública, ya que son redes con pocos nodos habilitados para acceder, comprobar y validar transacciones, se aprovechan de otras características de esta tecnología como puede ser la inmutabilidad, la transparencia a nivel interno, la seguridad y la rapidez de verificación de sus datos.

2. ASPECTOS JURÍDICOS DE LA TECNOLOGÍA BLOCKCHAIN:

La tecnología blockchain es una tecnología nueva que apenas lleva una década existiendo, concretamente, desde el 2009 cuando se validó el bloque génesis (primer bloque de transacciones) de la red de Bitcoin. Debido a este breve tiempo de vida, todavía no se le ha dotado de una regulación uniforme a sus principales aspectos que conllevan consecuencias jurídicas.

Posteriormente al nacimiento de la red de Bitcoin, se han creado numerosas redes blockchain en las que los criptoactivos son creados, almacenados y transferidos. El hecho de que las principales redes como la de Bitcoin, todavía no hayan alcanzado su objetivo de convertirse en un medio de pago, hace que la principal utilidad que se les está dando a los criptoactivos surgidos a partir de esta tecnología es la de constituirse como instrumentos de inversión. Las personas, en mercados secundarios de negociación de estos activos, valoran a los criptoactivos en función de la oferta y la demanda.

Actualmente, el criptoactivo con mayor capitalización de mercado es el *bitcoin* (tiene el mismo nombre que la red blockchain de la que procede) seguida del *ether* (criptoactivo nativo de la red de ethereum).

Los principales aspectos de la tecnología blockchain que generan consecuencias jurídicas, vienen de dos vertientes. Por un lado, tenemos los **casos de uso o**

aplicaciones de la tecnología blockchain y por el otro, tenemos a las consecuencias jurídicas que tienen las **características** de la tecnología.

La primera de las vertientes hace referencia a las aplicaciones actuales de la tecnología blockchain. Como ya se ha mencionado, la más conocida es la creación y transmisión, a través de la misma, de los criptoactivos (ya sean criptomonedas o tokens). Relacionado con los criptoactivos hay aspectos como las ICOs (Initial Coin Offering) como formas de obtener financiación con la emisión de criptoactivos en la creación de empresas que también tienen importantes implicaciones legales a considerar.

En definitiva, esta vertiente hace referencia a la economía que surge de las criptomonedas y los tokens y sus implicaciones en la naturaleza jurídica de los criptoactivos, en el ámbito fiscal, en el ámbito de la prevención del blanqueo de capitales o en el ámbito de los derechos de los consumidores de este tipo de criptoactivos

Asimismo, debido a que a partir de estas redes distribuidas, los llamados contratos inteligentes o *Smart contracts*, como se les llama en inglés (contratos autoejecutables sin intervención de terceros) se vuelven confiables, surgen multitud de usos gracias a estos, tal y como se explicó anteriormente, de manera que también habrá que entrar en la valoración de si los Smart contracts pueden llegar a ser o no contratos con consecuencias legales en la vida real.

La segunda de las vertientes hace referencia a las consecuencias jurídicas que surgen a partir de la propia tecnología blockchain en sí misma. Como se ha comentado anteriormente, la tecnología blockchain ofrece un nuevo paradigma en las transacciones de datos entre personas físicas o jurídicas, suprimiendo la necesidad de intermediarios y la necesidad de tener que confiar en la otra parte. Esto lo consigue gracias a las características de la descentralización y la inmutabilidad. La propia naturaleza de esta tecnología impide que un dato que ha sido introducido en la red se pueda eliminar ni modificar, algo que tiene evidentes consecuencias jurídicas en relación con la Protección de Datos Personales cuando se trate de personas físicas.

2.1. IMPLICACIONES JURÍDICAS DE LAS APLICACIONES DE LA TECNOLOGÍA BLOCKCHAIN:

A. Criptoactivos:

a) *¿Qué son?*

Los criptoactivos son representaciones digitales que representan activos o derechos que se construyen, transfieren y se almacenan en este tipo de bases de datos de registro distribuido¹². Utilizan cifrados criptográficos para garantizar su titularidad, asegurar las transacciones y controlar la emisión de los mismos.

Existen varios tipos de criptoactivos. En este trabajo, para facilitar la comprensión al lector medio, se va hacer la siguiente clasificación. Por un lado las **criptomonedas**, dentro de las cuales se diferencian dos clases: las que incorporan derecho de reembolso contra el emisor (las conocidas como stablecoins, las cuales están respaldadas por otros activos) y las que no incorporan tal derecho (como *bitcoin* y *ether*). Por otro lado, se encuentran los **tokens**, dentro de los cuales se engloban todos aquellos criptoactivos creados por empresas privadas para ofrecer utilidad a sus tenedores, ya sea en forma de retorno de inversión (en este caso, se tratará de tokens de seguridad o security tokens) o en forma de obtener derechos sobre bienes y servicios por la posesión del token (en este caso se tratará de tokens de utilidad).

En el grupo de las **criptomonedas**, las que incorporan derecho de reembolso contra el emisor son aquellas que están garantizadas mediante activos subyacentes, los cuales pueden ser de diversos tipos (monedas de curso legal, materias primas, activos tradicionales, acciones...). Además, estas son emitidas por sujetos identificables. La cuantía del reembolso al tenedor de estas criptomonedas es el valor patrimonial del activo subyacente al que esté emparejada.

Las que no incorporan tal derecho son criptomonedas como *bitcoin* y *ether* las cuales tienen el valor patrimonial resultante que se les atribuya en la negociación con las mismas en mercados secundarios. Algunas de este tipo no tienen un emisor identificable, pues, por ejemplo, en el caso de Bitcoin, su emisión se produce en forma de incentivo de forma autónoma como recompensa por mantener la llevanza de un algoritmo de código abierto¹³.

Lo que tienen en común las criptomonedas es su finalidad. Todas las criptomonedas surgen con la intención de convertirse en medios de pago generalizadamente aceptados.

Sin embargo, muchos activos digitales de los criptoactivos se han convertido en

¹² Artículo 3.1.2º de la Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937

¹³ SUAREZ PUGA, ERNESTO ALEJANDRO., «Naturaleza y régimen jurídico de las criptomonedas. », InDret 2.2021, p. 392

unidades de valor de cambio para numerosas transacciones. Así nacen los denominados *tokens*, los cuales pueden entenderse como unas fichas criptográficas representantes de unidades de valor¹⁴ dentro de una red blockchain y que pueden servir para la obtención de determinados beneficios tales como derechos, productos o servicios.

Dado que, por el momento, los criptoactivos como las criptomonedas no han conseguido el estándar de medio de pago generalmente aceptado, tal y como ya se ha comentado con anterioridad, la predominante utilidad que están teniendo estas son la utilización de dichos criptoactivos como instrumentos de inversión, los cuales se negocian en mercados secundarios donde se compran y venden las criptomonedas y los diferentes tokens con expectativas de revalorización en su precio referenciado a una moneda fiduciaria¹⁵ (euro, dólar...). De la misma forma los tokens también pueden ser negociados en este tipo de mercados secundarios y así ser empleados meramente como instrumentos financieros.

Los agentes que intervienen en este tipo de mercados secundarios son los siguientes:

- **Compradores y vendedores de criptoactivos:**

Los compradores de criptoactivos adquieren este tipo de activos para obtener diversas utilidades o para venderlos cuando los mismos se revaloricen. Los vendedores de criptoactivos pueden ser bien los emisores de los mismos, como puede ser el caso de los mineros por ejemplo en la red de bitcoin, o los creadores de un token. Sin embargo, también pueden ser usuarios que habían sido compradores en su momento y ahora los venden.

Esas compras y ventas de criptoactivos se pueden hacer a través de varias vías o canales de intercambio, como puede ser la venta a otra persona mediante una transferencia persona a persona (P2P), a través de plataformas de negociación de criptoactivos de manera descentralizada o a través de servicios de cambio de criptoactivos por monedas de curso legal.

¹⁴FUENMAYOR, CARLOS «Criptoactivos: un nuevo activo de inversión» en *Instituto de Estudios Financieros*, párrafo 11, febrero 2022.

¹⁵ SUAREZ PUGA, ERNESTO ALEJANDRO., «Naturaleza... *cit.*, p. 393

- **Proveedores de servicios de cambio de criptoactivos por dinero de curso legal:**

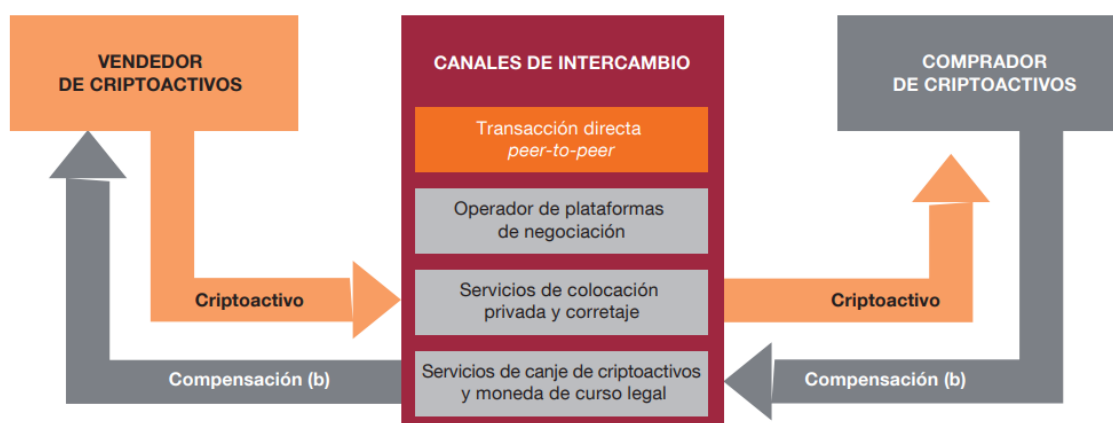
Son los denominados exchanges. Estos se encargan de actuar como punto de encuentro entre compradores y vendedores. En ellos, se realizan intercambios de monedas de curso legal por criptoactivos o intercambios entre criptoactivos.

- **Proveedores de custodia de criptoactivos:**

Como ya se ha mencionado, los criptoactivos no existen de manera física, como sí lo hacen las monedas de curso legal. En contraposición a su existencia física, los criptoactivos se almacenan en carteras digitales, donde se pueden guardar, enviar o recibir este tipo de activos. No son más que un software que almacena las claves que dan propiedad y derecho sobre los criptoactivos. De esta manera, si las claves que dan derecho a almacenar una criptomoneda son robadas, no hay manera de recuperar dichas criptomonedas, ya que a causa de la descentralización no existe ninguna entidad central a la que se pueda acudir en este tipo de situaciones¹⁶.

En definitiva, el flujo de los criptoactivos se realiza siguiendo el siguiente esquema que definió el Banco de España en su informe especial sobre criptoactivos y sus riesgos para la estabilidad financiera de la economía española¹⁷.

AGENTES PARTICIPANTES EN LOS MERCADOS DE CRIPTOACTIVOS (a)



Fuente: Banco de España

¹⁶ Banco Santander: Guía para saber que son las criptomonedas. Disponible en: <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas> (Consulta: 10 de abril 2022)

¹⁷ BANCO DE ESPAÑA «Especial. Criptoactivos» *Informe de estabilidad financiera. Primavera 2022*, p. 156.

b) Normativa y retos jurídicos:

- **Naturaleza jurídica de los criptoactivos:**

La definición más reciente de criptoactivo a nivel comunitario la hizo la Comisión Europea, la cual, con la finalidad de proponer un marco regulatorio homogéneo para toda la Unión Europea, presentó en septiembre de 2020 la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos, más conocida como **ley MiCA**¹⁸. En la mencionada propuesta, se hizo una definición de los criptoactivos que viene a decir lo siguiente: “un criptoactivo es una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar”.

Sin embargo, con esta definición no se aclara cual es la naturaleza jurídica de estos activos, cuestión fundamental para establecer los límites regulatorios.

A continuación, con base en la clasificación sobre posibles figuras jurídicas en las que las criptomonedas podrían encajar, realizada por la profesora Dra. M^a Concepción Chamorro Domínguez¹⁹ se analizarán algunas de esas figuras jurídicas en las que los criptoactivos serían susceptibles de enmarcarse, con la advertencia de que, tal y como se ha comentado anteriormente, existen diversas clases de criptoactivos.

Medio de pago

Algunos criptoactivos, como es el caso de las criptomonedas, nacieron con la finalidad de ser medios de pago, sin embargo, en la actualidad la calificación legal de los criptomonedas como medio de pago de curso legal todavía no se ha dado. En este sentido, la Directiva 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, en su modificación por la Directiva 2018/843, define a las monedas virtuales como: *representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no asociada a una moneda establecida legalmente, que **no posee el estatuto de moneda o dinero**, pero aceptada por personas físicas o jurídicas*

¹⁸ Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937

¹⁹ CHAMORRO DOMÍNGUEZ, M^a DE LA CONCEPCIÓN, «Aspectos jurídicos de las criptomonedas». Disponible en: https://blockchainintelligence.es/wp-content/uploads/2019/04/Art%C3%ADculo-doctrinal_Apectos-jur%C3%ADficos-de-las-criptomonedas-por-M-de-la-Concepci%C3%B3n-Chamorro-Rodr%C3%ADguez.pdf (Consulta: 25 de abril 2022)

*como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*²⁰.

A nivel nacional, recientemente, la CNMV ha seguido con la postura de la Comisión Europea y en un comunicado junto con el Banco de España en el que advierten de los riesgos vinculados a invertir en este tipo de activos²¹, remarca que las criptomonedas no son medio de pago de curso legal y que su emisión no está garantizada por ningún Banco Central.

Sin embargo han habido sentencias, tanto a nivel europeo como a nivel nacional que a pesar de excluirlas de esa categorización, sí que los encuadran en la categoría de **medio de pago de curso no legal**, es decir, vienen a destacar que, siempre y cuando en una transacción bilateral las partes acepten, las criptomonedas pueden ser utilizados como medio de pago o medio de intercambio.

A nivel comunitario, se trata de la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Quinta) de 22 de octubre de 2015 en el asunto C-264/14²², la cual viene a decir que el *bitcoin*, cuando se utiliza como medio de pago por acuerdo entre las partes, se asemeja a las monedas tradicionales a efectos de IVA, pues considera que la finalidad es la misma, esto es, la de ser un medio de pago.

A nivel nacional, también el Tribunal Supremo se pronunció en su Sentencia 326/2019 de 20 de junio del Tribunal Supremo²³, en la que definió al *bitcoin* como un activo inmaterial, una unidad de cuenta de la red blockchain en la que se emiten y por tanto no pueden ser considerados medios legales de pago o instrumentos de dinero electrónico. Sin embargo, destacó en dicha sentencia el Tribunal Supremo que, al tener el *bitcoin* precios de compra y de venta que suelen coincidir debido a las leyes de la oferta y la demanda, nada impide que dichos activos inmateriales puedan usarse como medio de intercambio siempre y cuando las partes de la transacción de que se trate estén de acuerdo.

²⁰ Art. 1.2).d) de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

²¹ Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión de fecha 9 febrero de 2021. Disponible en: <https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D> (Consulta: 21 de marzo de 2022)

²² Sentencia del Tribunal de Justicia (Sala Quinta) de 22 de octubre de 2015. Asunto C-264/14. Base de datos: Curia. Disponible en: <https://curia.europa.eu/juris/liste.jsf?td=ALL&language=es&jur=C,T,F&num=C-264/14>

²³ Sentencia del Tribunal Supremo 326/2019, 20 de Junio de 2019. Base de datos: vLex. Disponible en: <https://vlex.es/vid/797938401>

Bien mueble digital:

Otra de las categorías en la que pueden encajar los criptoactivos, son la de un bien mueble digital. Como se ha señalado en el apartado anterior, las criptomonedas no se pueden considerar medios de pago de curso legal, sin perjuicio de que, de mutuo acuerdo, las partes acepten establecer como medio de pago a estos, de manera que actuarían como medios de pago análogos a los de curso legal.

La consideración de los criptoactivos como bien mueble digital viene de la constitución de sociedades de capital con uno de ellos, concretamente con la criptomoneda *bitcoin*. Dado que su naturaleza no permitía considerarlos como aportación monetaria, el notario encargado de inscribir en el Registro Mercantil la escritura de constitución²⁴, consideró a los bitcoins como aportaciones no dinerarias considerando que cumplían con el requisito para serlo que establece el artículo 58.1 de la Ley de Sociedades de Capital²⁵ de que todos los bienes que se aporten en la constitución de una sociedad han de ser susceptibles de valoración económica.

Además el artículo 63 de la Ley de Sociedades de Capital establece que en la escritura de constitución deberán describirse las aportaciones no dinerarias con sus datos registrales si existieran, la valoración en euros que se les atribuya, así como la numeración de las acciones o participaciones atribuidas. Para cumplir con estas estipulaciones el Notario encargado de dar fe pública de esta escritura definió a bitcoin como *“un bien patrimonial inmaterial “documento electrónico”, objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada “Bitcoin”, que permite ser utilizada como contraprestación en transacciones de todo tipo.”* Por ello, en la escritura se aportó la valoración económica en euros de la cantidad determinada de bitcoins que se aportaron en ese momento y la dirección de la cartera a la que se transfirieron los bitcoins, junto con la clave pública a la que esta última estaba vinculada. Los bitcoin objeto de la aportación ahora pasaban a ser propiedad de la sociedad creada.

La consideración de los criptoactivos como bienes muebles digitales para su consideración como aportaciones no dinerarias en la constitución de sociedades necesitarán entonces de una valoración razonable de la aportación realizada, una descripción del aporte realizado (dirección electrónica de la cartera digital en la que se

²⁴ GOMA LANZÓN, IGNACIO., «¿Se puede constituir una sociedad con bitcoins?» Blog de Hay Derecho, de 9 de junio de 2014. Disponible en: <https://www.hayderecho.com/2014/06/09/se-puede-constituir-una-sociedad-con-bitcoins/> (Consulta: 22 de abril 2022)

²⁵ Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital. (LSC)

alojan, junto con su clave pública) y una determinación del número de criptoactivos aportados.

Instrumento financiero o valor negociable:

Como se ha explicado en la clasificación realizada de los tipos de criptoactivos, los hay que no tienen la finalidad de convertirse en divisas digitales y cumplir así como instrumentos de pago. Concretamente, se trata de los tokens de utilidad (utility tokens) y de los tokens de seguridad (security tokens). Estos tokens pueden servir como instrumentos de inversión.

Los primeros dan derecho a acceder a un servicio o a recibir un producto, en principio, no están pensados para ser utilizados para bienes de inversión, eso no quita que en función de la oferta y la demanda estos tipos de criptoactivos puedan ser negociados en mercados no regulados con expectativas de obtener liquidez por los vendedores de los mismos. Los segundos generalmente otorgan participación en los beneficios o en los futuros ingresos y aumentos de valor de la entidad que los emite²⁶.

Sin embargo, para que se traten de valores negociables y con ello, estar sujetos a la normativa europea y nacional, la Comisión Nacional del Mercado de Valores (CNMV) en un comunicado sobre criptomonedas e ICOs para profesionales del sector financiero²⁷, como se explicará detalladamente en el siguiente punto, estableció que para que un criptoactivo como un token pueda considerarse valor negociable se tiene que dar una correlación expresa entre la adquisición del criptoactivo y sus expectativas de revalorización o de obtención de beneficios gracias al mismo.

- **Control de la emisión de criptoactivos:**

La Ley del Mercado de Valores²⁸ establece que los instrumentos financieros que puedan ser englobados en los que en su artículo 2 se detallan, tienen que ser autorizados para su

²⁶ Comunicado conjunto de la CNMV y del Banco de España sobre “criptomonedas” y “ofertas iniciales de criptomonedas” (ICOs) de fecha 8 febrero 2018. Disponible en: https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07.pdf (Consulta: 26 marzo 2022)

²⁷ Consideraciones de la CNMV sobre “criptomonedas” e “ICOs” dirigidas a los profesionales del sector financiero de 8 de febrero de 2018. Disponible en: <http://www.cnmv.es/Portal/verDoc.axd?t=%7b9c76eef8-839a-4c19-937f-cfde6443e4bc%7d> (Consulta: 26 marzo 2022)

²⁸ Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores. (TRLMV)

emisión por la CNVM, así como someterse a su supervisión. En relación con los criptoactivos, dichas implicaciones jurídicas se deberán tener en cuenta a la hora de llevar a cabo la emisión de los mismos.

Para analizar los aspectos jurídicos de las emisiones de criptoactivos por empresas privadas, hay que tener en cuenta la distinción que se ha explicado en el punto anterior entre los **utility tokens** y los **security tokens**.

La CNMV, estima que para que a un token se le dé la categoría de valor negociable, se tiene que dar una **correlación directa** entre la adquisición del mismo y las expectativas de adquirir derechos o expectativas de participación en la potencial revalorización o rentabilidad de negocios o proyectos o, en general, que presenten u otorguen derechos equivalentes o parecidos a los propios de las acciones, obligaciones u otros instrumentos financieros incluidos en el artículo 2 del TRLMV. O, por otra parte, que den derecho a acceder a servicios o a recibir bienes o productos, que se ofrezcan haciendo referencia, explícita o implícitamente, a la expectativa de obtención por el comprador o inversor de un beneficio como consecuencia de su revalorización o de alguna remuneración asociada al instrumento o mencionando su liquidez o posibilidad de negociación en mercados equivalentes o pretendidamente similares a los mercados de valores sujetos a la regulación. En definitiva, tiene que existir un ánimo de lucro mediante la revalorización de los derechos que otorga un token para que éste sea considerado valor negociable.

Los **utility tokens**, al no poder considerarse valores negociables porque no cumple con los requisitos de la CNMV para que exista esa correlación entre adquisición del criptoactivo en cuestión y sus expectativas lucrativas, no necesitan de autorización de la CNMV para ser emitidos mientras que los **security tokens** son considerados activos financieros y por ello están sometidos a la normativa financiera nacional y comunitaria y sí que necesitan de la supervisión y de la autorización de la CNMV para ser emitidos.

Así, los denominados security tokens entran dentro del marco regulatorio de la Directiva Europea sobre los Mercados de Instrumentos Financieros (MiFID II) y de la Ley del Mercado de Valores. Dichos tokens tendrán, por tanto, un régimen que protege más al inversor al estar negociados en mercados regulados. También tendrán que cumplir con la normativa Anti-money Laundering (AML), una normativa que persigue

desincentivar el fraude y con la normativa Know Your Customer (KYC), la cual obliga a que todos los inversores estén correctamente identificados²⁹.

- **Derechos de los consumidores y usuarios: obligaciones de información y transparencia sobre los riesgos que conllevan.**

En este sentido no existe todavía una protección de los consumidores similar a la que tienen en otros aspectos. Solo existe la Circular de la CNMV sobre publicidad de criptoactivos de 10 de enero de 2022³⁰. En ella, se definen las reglas sobre el contenido y el formato que los mensajes publicitarios de las campañas sobre criptoactivos presentados como bienes de inversión tienen que tener.

El principal objetivo que quiere cumplir la CNMV, es que queden claros para los consumidores y usuarios los riesgos afectos en la inversión en este tipo de activos y para conseguirlo la publicidad se debe ofrecer de una forma equilibrada en la que se den contenidos objetivos, veraces, no engañosos e imparciales. Obliga a que todas aquellas ofertas relacionadas con estos han de incluir la siguiente advertencia: *“La inversión en criptoactivos no está regulada, puede no ser adecuada para inversores minoristas y perderse la totalidad del importe invertido”*. Además, se proporcionarán enlaces para que las personas puedan acceder a observar informes con la cantidad de riesgos que conllevan.

En la Circular, se establece que todas aquellas ofertas publicitarias relacionadas con criptoactivos que vayan destinadas a más de 100.000 personas deben contar con una comunicación previa a la Comisión Nacional de Mercados y Valores al menos antes de 10 días a que la campaña publicitaria tenga lugar.

En definitiva, se trata de imponer a los proveedores de criptoactivos una serie de obligaciones de información precontractual con la finalidad de que los consumidores de estos puedan hacerse una representación mental lo más precisa posible sobre los riesgos que conllevan.

²⁹ TERSTIEGE ORTIZ, MANUEL. «Aspectos jurídicos a tener en cuenta en la emisión de criptoactivos por la empresa (utility token vs security token)» *DPO&it law*, 26 de octubre de 2021.

³⁰ Nueva Circular de la CNMV de publicidad sobre criptoactivos presentados como objeto de inversión. *Nota de prensa*, 21 de enero de 2022. Disponible en: <https://www.cnmv.es/portal/verDoc.axd?t={67a4f7e8-49b7-42ec-8328-f8f4b2004cd8}>.

- **Prevención blanqueo de capitales:**

A pesar de que una de las características de la tecnología blockchain sea la transparencia y trazabilidad de sus transacciones, hay que destacar que el hecho de que se puedan rastrear transacciones no implica que se conozca quien está detrás de cada transacción, pues las transacciones visibles en blockchain se representan mediante envíos de carteras digitales a carteras digitales y éstas están identificadas mediante códigos (claves públicas) que no en todos los casos se tiene por qué conocer quién está detrás de cada cartera digital. Es por esto, que se dice que blockchain permite cierta anonimidad a sus usuarios al trabajar estos con claves públicas que, si no es obligatorio identificarlas, no se pueden atribuir a ninguna persona en concreto.

Esto es una característica que puede conllevar actuaciones fraudulentas difíciles de rastrear. Ante este problema, la Directiva 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, introduce, tras su modificación por la Directiva 2018/843 los nuevos apartados 18 y 19 que definen “monedas virtuales” y “proveedor de servicios de custodia de monederos electrónicos”³¹. De esta manera, obliga a los proveedores de servicios de cambio de criptoactivos por dinero de curso legal y a los proveedores de custodia de criptoactivos a cumplir con las estipulaciones de la Directiva. Concretamente se imponen a estos sujetos obligaciones como la necesidad de estar inscritos en los Registros correspondientes, la identificación de todos sus usuarios y que reporten de operaciones sospechosas.

A nivel nacional, esta Directiva se traspone al ordenamiento español a través del Real Decreto-ley 7/2021, de 27 de abril³², por el que se modifica, entre otras, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo³³. Con esta modificación se prevé que los nuevos sujetos obligados estén

³¹ Art. 1.2).d) de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849... *cit.*

“monedas virtuales”: representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos;

“proveedor de servicios de custodia de monederos electrónicos”: una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales.».

³² 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.

³³ Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. (LPBCFT)

adscritos al régimen de diligencia debida con el objetivo de prevenir el fraude fiscal y la financiación del terrorismo.

En sus artículos 3 y ss. establece la obligación de la **identificación** formal de todas las personas físicas o jurídicas que creen relaciones de cualquier índole con los sujetos obligados, es decir, se requiere la identificación formal de todos aquellos sujetos que lleven a cabo negocios o cualquier clase de relación jurídica con proveedores y/o guardadores de criptoactivos. También se informará de la titularidad real de los criptoactivos, y se llevará un seguimiento continuo de los titulares.

Es en la Disposición Adicional Segunda de la LPBCFT donde se establece la obligación de que los sujetos que realicen actividades relacionadas con el intercambio de criptoactivos por monedas de curso legal o con la custodia de los mismos, tendrán que inscribirse en un **Registro**³⁴ creado a tal efecto en el Banco de España. Para conseguir dicho registro se tendrán que cumplir con los requisitos de honorabilidad comercial y profesional prevista para las entidades de crédito. Requisitos que aparecen mencionados en el artículo 30 del Real Decreto 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito³⁵, y que hacen referencia a cuestiones como la buena conducta profesional que se haya venido mostrando durante la vida profesional de la entidad en cuestión, la cual se valorará atendiendo a su trayectoria así como a la ausencia de infracciones. Además, para conseguir el registro, los sujetos obligados deberán contar con **procedimientos y órganos internos de supervisión** previstos en los artículos 26, 26 bis y 26 ter de la LPBCFT con el fin de que adviertan sobre operaciones sospechosas y así conseguir una correcta prevención del blanqueo de capitales y de la financiación del terrorismo.

En España, están registrados en el Registro creado a tal efecto en el Banco de España como proveedores de servicios de cambio de moneda virtual por moneda de curso legal o como entidades que se encargan de la custodia de criptoactivos un total de 7 entidades, 5 de ellas españolas.

³⁴ Banco de España: Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Disponible en: https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html (Consulta: 12 de mayo de 2022)

³⁵ Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. (LOSSEC)

- **Encaje fiscal de los criptoactivos:**

Los criptoactivos, como se ha comentado anteriormente, todavía no tienen una naturaleza jurídica consolidada a nivel comunitario ni a nivel nacional. Es por ello que a la hora de establecer su tributación, no se sabe con certeza a que categoría de la legislación sobre impuestos actual pertenecen. Será con la Ley MiCA con la que se alcanzará esa seguridad jurídica a nivel comunitario necesaria para poder hablar en términos absolutos y homogéneos sobre el alcance tributario de los criptoactivos. Sin embargo, es previsible que dicha normativa tarde todavía unos años hasta su aprobación, por ello, hasta ahora, las únicas conclusiones en materia de tributos sobre los criptoactivos que han sido dadas son las que ha ido haciendo la Dirección General de Tributos en sus consultas vinculantes, por lo que de momento es a lo que habrá que acogerse.

1. IRPF:

En relación con el Impuesto sobre la Renta de las Personas físicas, la Dirección General de Tributos ha llevado a cabo diversas consultas vinculantes en las que considera que las ventas de criptoactivos a cambio de moneda de curso legal o las permutas de criptoactivos son susceptibles de generar ganancias o pérdidas patrimoniales imputables a la base del ahorro. Siempre y cuando estas actuaciones se lleven a cabo al margen de una actividad económica o profesional.

Concretamente, en la consulta V1149-18³⁶ en la que se pedía a la DGT que se pronunciara sobre qué efectos producen las rentas derivadas de la venta de criptomonedas por euros y sobre qué calificación tienen los intercambios entre criptomonedas, la DGT definió a las monedas virtuales como bienes inmateriales, computables por unidades o fracciones de unidades que pueden ser intercambiadas por otros bienes, incluso por monedas de curso legal si así lo pactan las partes en una transacción.

Con respecto a la primera cuestión, la DGT destacó que cuando una criptomoneda se vende por moneda de curso legal, en este caso, en euros, se produce una alteración patrimonial equivalente a la diferencia entre el valor de adquisición de la criptomoneda y el valor de transmisión con la venta, la cual será considerada una ganancia patrimonial

³⁶ DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V2679-21 de 5 de noviembre de 2021. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/> (Consulta 16 mayo 2022)

si el valor de adquisición es menor que el de transmisión, y una pérdida patrimonial si el valor de transmisión es menor que el valor de adquisición. Por tanto, se tratará de una renta que computará en la base imponible del ahorro con unos tipos de entre el 19% y el 26%, sin perjuicio de que dicha actividad se realice en el marco de una actividad económica en cuyo caso, dicha renta computaría en la base imponible general.

Respondiendo a la segunda cuestión, la Dirección General de Tributos consideró que el intercambio de una criptomoneda por otra constituía una permuta tipificada en el artículo 1.538 del Código Civil (contrato por el cual cada uno de los aportantes se obliga a dar una cosa para recibir otra). De esta manera al intercambiar una con otra habrá que atender a cuál ha sido la alteración patrimonial que haya tenido lugar y será esa alteración la que se califique como ganancia o pérdida patrimonial de acuerdo con lo dispuesto en el art. 33.1 de la Ley del Impuesto sobre la Renta de las Personas Físicas³⁷. Para la valoración se deberá tomar la diferencia entre el valor de adquisición se la criptomoneda entregada y el mayor valor de los dos siguientes: el de la criptomoneda recibida o el de la criptomoneda entregada a cambio, todo ello conforme a lo que establece el art 37.1.h) de la LIRPPF.

2. IVA:

Son varias las consultas que han tenido lugar en relación a la sujeción al Impuesto Sobre el Valor Añadido de los servicios relacionados con criptoactivos, ya sean servicios de cambio de moneda virtual por moneda de curso legal o de servicios de custodia de criptoactivos.

Una de las más recientes es la Consulta V2679-21³⁸ con fecha de 5 de noviembre del 2021. En ella, la consultante era un sujeto que prestaba servicios de custodia de criptomonedas, compraventa de las mismas en un mercado no regulado y servicio de staking o rentabilidad por el hecho de depositarlas en un Smart contract. Consultaba por la sujeción o exención al Impuesto de las actividades mencionadas.

³⁷ Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio (LIRPF).

³⁸ DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V1149-18 de 8 de mayo de 2018. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/> (Consulta: 16 mayo 2022)

En primer lugar, la DGT se pronuncia sobre la sujeción o no y, en su caso, exención del servicio de compraventa de criptoactivos. Su respuesta se basa en el criterio con el que consideró el Tribunal de Justicia de la Unión Europea al Bitcoin y al resto de criptomonedas en su sentencia de 22 de octubre de 2015, David Hedqvist, asunto C-264/14. En ésta, el TJUE, consideró al bitcoin y al resto de criptomonedas como divisas virtuales y en el apartado 53, concluyó que los servicios financieros relacionados las mismas entran dentro de los servicios exentos al IVA a que se refiere el artículo 135.1.e) de la Directiva del IVA³⁹. Concretamente, a nivel nacional, dichos servicios financieros con divisas virtuales quedan exentos del impuesto en el art. 28.Uno.18ª.j) de la Ley de IVA⁴⁰. En conclusión, la prestación de servicios de compra y venta de criptoactivos en mercados no regulados queda sujeta y exenta al Impuesto Sobre el Valor Añadido.

En segundo lugar, en cuanto a la sujeción o no y la exención o no de la **prestación de servicios de custodia de criptoactivos**, la DGT distingue entre la custodia en carteras digitales frías y carteras digitales calientes⁴¹. En este sentido, se hace referencia a que las carteras que no están conectadas a internet (proporcionan mayor seguridad) se asimilan al alquiler de cajas de seguridad, por lo que esta actividad está sujeta y no exenta de IVA en base al artículo 135.2.d) de la Directiva del IVA y a la conclusión con la misma fundamentación jurídica que ya hizo la DGT sobre la prestación de servicios de alquiler de cajas de seguridad en una Resolución de 1987.

Por último, se hace referencia a la cuestión sobre la sujeción al IVA de la **prestación del servicio de proveedor de staking**⁴² a través de un contrato inteligente. Antes de entrar en el asunto, la DGT hace la distinción entre la propia actividad del staking y la de ofrecer servicios de staking.

En la primera de ellas una persona bloquea sus criptomonedas en una billetera digital para tener posibilidades de ser elegido aleatoriamente para validar un bloque de transacciones y obtener rentabilidad con ello. Los rendimientos obtenidos de esta actividad tienen naturaleza financiera pues son análogos a los derivados de la cesión de

³⁹ Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido

⁴⁰ Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido. (LIVA)

⁴¹ Wallet fría: cartera digital no conectada a internet vs. wallet caliente: cartera digital conectada a internet.

⁴² Servicio de proveedor de staking: a través de un Smart contract, el proveedor de este servicio, a cambio de unas comisiones, permite a los usuarios aportar fondos a dicho contrato para obtener fracciones de rentabilidad del nodo validador. Se trata de una cesión de fondos a un nodo validador, mientras que en la propia actividad de staking la persona que bloquea los fondos es el propio nodo validador.

bienes a terceros y por tanto quedan sujetos y exentos de IVA (art. 20.Uno.18ª Ley del IVA). Tributarán en la base imponible general del IRPF si se hacen de forma profesional y en la base imponible del ahorro si no son obtenidos resultado de una actividad profesional.

Sin embargo, en la segunda, el proveedor de servicio de staking gracias a un contrato inteligente, recibe rendimientos proporcionales a la rentabilidad obtenida por los usuarios. Al tener estos rendimientos una naturaleza no financiera, la Dirección General de Tributos concluye que los servicios prestados como proveedor de staking quedan sujetos y no exentos de IVA.

Otra de las consultas más recientes que se han hecho a la Dirección General de Tributos es la que lleva por número V0486-22⁴³. Esta consulta versa sobre la tributación al Impuesto Sobre el Valor Añadido de la venta de NFT⁴⁴ (No Fungible Tokens) por una persona física.

En dicha consulta la Dirección General de Tributos, ante la falta de pronunciamientos por parte del Tribunal de Justicia de la Unión Europea sobre la naturaleza jurídica de este tipo de criptoactivos, lleva a cabo un análisis de esa naturaleza con el objetivo de determinar si nos encontramos ante una entrega de bienes o una prestación de servicios. En primer lugar, determina que lo que se negocia en una compraventa de un NFT, es el token que representa una creación artística digital, no la titularidad del archivo digital subyacente. Dicho token tiene una naturaleza no fungible por el hecho de que es único e irrepetible, es decir, es un activo digital no intercambiable por otro que solo existe uno y no otro igual que representa cualquier archivo digital subyacente (creación musical o artística, una pieza de video, una imagen...). Se pueden asemejar a certificados de autenticidad digitales de la obra que representan y por ello la Dirección General de Tributos, entiende que la actividad que está llevando a cabo la persona física consultante consistente en la venta de NFTs, puede asemejarse a un servicio de prestación de certificados de autenticidad sobre archivos digitales existentes en internet y por tanto accesibles a todo el mundo.

Concluye por tanto que la actividad prestada por el consultante es calificada como una prestación de servicios prestada electrónicamente y que por tanto deberá tributar al tipo general del 21% de IVA siempre y cuando comprador y vendedor residan en territorio nacional.

⁴³ DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V0486-22 de 10 de marzo de 2022. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/> (Consulta: 16 mayo 2022)

⁴⁴ NFT: se trata de un tipo de token que es único y exclusivo. También es no fungible: no consumible.

3. IP:

En relación con el Impuesto sobre el Patrimonio varias han sido las consultas a la DGT sobre cómo han de computarse las tenencias de criptoactivos, ya que al poder considerarse estos como medio pago en una transacción en la que las partes acepten, podría tener un tratamiento similar a la tenencia de una divisa tradicional y entrar dentro del hecho imponible de este impuesto. Además, el hecho de que estos activos puedan ser negociados en mercados no regulados hace que estos activos puedan entrar dentro del hecho imponible, ya sea por una vía o por la otra.

La opción por la que ha optado la Dirección General de Tributos en este aspecto es la de la declaración de los criptoactivos de forma análoga a la de otras divisas tradicionales. La valoración que deberá darse a los criptoactivos es la que tengan a fecha 31 de diciembre, pues es esta la fecha en la que este impuesto tiene su devengo. La valoración deberá estar hecha en euros, tal y como se indica en Consulta Vinculante V0590-18⁴⁵.

B. Smart contracts:

a) ¿Qué son?

Otra de las aplicaciones más conocidas que la tecnología blockchain ha favorecido, es el desarrollo de Smart contracts. Antes de adentrarse en los retos jurídicos de este tipo de contratos, se hace necesario definir qué se entiende por Smart Contract o contrato inteligente. Este tipo de contrato no es más que un acuerdo cuyas condiciones se redactan en lenguaje de código informático y se auto ejecutan automáticamente cuando se cumple lo estipulado en el acuerdo. Se trata de un programa que digitaliza las cláusulas pactadas del contrato y cuando sucede un acontecimiento previsto en el contrato es capaz de procesar esa información para auto ejecutar la consecuencia de ese evento ocurrido⁴⁶.

Gracias a los Smart Contracts, es posible contratar con personas desconocidas sin tener que confiar en la honorabilidad de la contraparte. Se tratan de códigos informáticos que son capaces de hacer cumplir acuerdos de voluntad entre desconocidos a través de internet sin necesidad de emplear un intermediario.

⁴⁵ DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V0590-18 de 1 de marzo de 2018. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/> (Consulta: 16 mayo 2022)

⁴⁶ BBVA Research: *Smart Contracts: ¿lo último en automatización de la confianza?*. Disponible en (link para descargar pdf): <https://www.bbva.com/es/smart-contracts-contratos-basados-blockchain/> . Consulta: 17 de mayo 2022.

Todo parte de un acuerdo a través del cual las partes deciden someterse a unas condiciones preestablecidas a partir de las cuales se producirán unas consecuencias también pactadas. Tienen una lógica funcional del tipo “si pasa X entonces Y”⁴⁷.

Por ejemplo, aplicando la lógica de los Smart contracts a un contrato de seguros por retraso o cancelación de vuelos, cuando se da el retraso o la cancelación cubiertos en la póliza, a través de un contrato de este tipo se podría automatizar la ejecución del pago al asegurado. En el ejemplo, a partir de la información de que el evento ha tenido lugar, se auto ejecutaría el pago al asegurado.

Ahora bien, sí que es cierto que el software de un Smart contract puede verificar toda aquella información que está dentro de la red blockchain en la que esté operando. Sin embargo el problema viene cuando se tiene que introducir información de la vida real, es decir, información no alojada en la blockchain para dar cumplimiento a las estipulaciones del contrato. Para solucionar este problema e introducir la información que tiene lugar en la vida real a la red blockchain, se utilizan los denominados oráculos, que son fuentes de información externas a la blockchain a partir de las cuales se consigue la información requerida por el Smart contract⁴⁸. Estos oráculos pueden ser de varios tipos, ya sean páginas web, empresas terceras, periódicos digitales o incluso sensores electrónicos conectados a internet⁴⁹.

Por ejemplo, en el ejemplo mencionado, el oráculo sería la controladora de vuelos AENA, la cual proporcionaría al Smart contract la información de que la cancelación ha tenido lugar, y automáticamente se ejecutaría el reembolso al asegurado.

También existen los oráculos descentralizados con el fin de evitar que el uso de una única fuente de información externa para conectar al mundo real con el digital actúe negligentemente y manipule dicha información. Dichos oráculos descentralizados hacen un análisis de todas fuentes de información existentes y toman la decisión de lo que dice la mayoría de ellas.

⁴⁷ PORXAS, N. y CONEJERO, M., “Tecnología blockchain... *cit.* p. 31.

⁴⁸ Bit2Me Academy: *¿Qué son los oráculos blockchain?*. Disponible en: <https://academy.bit2me.com/que-es-oraculos-blockchain/> (Consulta: 17 mayo 2022)

⁴⁹ FETSYAK, I. “Contratos inteligentes... *cit.* p.210-211

Aplicación de la lógica empresarial con los *smart contracts*



Fuente: BBVA Research

Son figuras que existían con anterioridad a la aparición de la tecnología blockchain (los creó Nick Szabo alrededor de 1994), pero sin la tecnología blockchain no tenían sentido porque a pesar de que sí que libran a las partes el tener que confiar entre ellas, había que confiar en la seguridad e incorruptibilidad del programa informático.

Ahora bien, es gracias a la aparición de la tecnología blockchain cuando este tipo de contratos cobran importancia (pues las instrucciones del contrato, al ser almacenadas en una red blockchain, se vuelven inmutables). Esto es porque gracias a las redes distribuidas y sus características de inmutabilidad y descentralización, cuando un Smart contract se introduce en una cadena de bloques, éste se vuelve invariable y puede ser cotejado por todos los nodos de la red en la que esté incrustado que las condiciones del contrato se hayan cumplido.

Con contratos de este tipo se pueden agilizar numerosos procesos gracias a la eliminación de intermediarios. Sin embargo deben ser cláusulas que no requieran interpretación, es decir, cláusulas de verificación objetiva.

b) Normativa y retos jurídicos:

Actualmente no existe ninguna ley reguladora específica de los contratos inteligentes. Por tanto, hay que remitirse a la legislación actual en materia de contratación y llevar a

cabo un análisis para dilucidar si los Smart contracts pueden contar con los aspectos jurídicos con los que cuentan los contratos tradicionales y así, producir efectos jurídicos en la vida real.

Los contratos definidos como contratos inteligentes presentan problemas en cuanto a su validez jurídica en la vida real. Para llevar a cabo un análisis de esta validez jurídica en primer lugar hay que hacer una valoración sobre la validez formal. Desde este punto de vista, los contratos inteligentes no se pueden calificar como contratos verbales, por lo que se calificarán como contratos escritos. Su redacción está realizada en forma de código informático, lo cual no es un impedimento pues en el ordenamiento español, porque tal y como indica el artículo 1278 del Código Civil⁵⁰, impera el principio de libertad de forma en la contratación, sin perjuicio de que existan materias en las que la forma sí que sea un requisito para determina la validez jurídica del contrato en cuestión, como por ejemplo puede ser el caso de los contratos celebrados con consumidores donde la forma escrita es un requisito de validez.

Más allá del ámbito formal, los contratos tienen que cumplir otra serie de requisitos para obtener la validez jurídica. A falta de una regulación existente en esta materia, los contratos a los que los Smart contracts se pueden asemejar son a los contratos electrónicos, ya que, en realidad son acuerdos de voluntad redactados y almacenados en computadoras.

Partiendo de esta base, hay que acudir a la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico⁵¹ y en esta, se observa en su artículo 23 que para que un contrato celebrado por vía electrónica produzca efectos jurídicos, ha de constar el consentimiento y los demás requisitos de validez de los contratos, los cuales aparecen en el artículo 1261 del Código Civil (consentimiento, objeto y causa).

En cuanto al **objeto**, el mencionado artículo 1261 del Código Civil establece que éste ha de ser un objeto cierto. La doctrina mayoritaria interpreta que el objeto cierto son todas aquellas realidades materiales, ya sean físicas o jurídicas, a las que las partes hacen recaer su consentimiento. Este requisito quedaría cumplido puesto que el código informático es una realidad con entidad material, ya que a pesar de no tener soporte físico como puede ser un papel, sí que cuenta con un soporte digital identificable.

⁵⁰ Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

⁵¹ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (LSSICE)

Los artículos 1271, 1272 y 1273 del Código Civil, establecen, además que el objeto tiene que ser lícito, determinable y recaer sobre cosas que no sean imposibles. En este sentido, habría problemas con el requisito que requiere que el objeto ha de ser lícito, pues, como se ha comentado en esta obra, la tecnología blockchain es susceptible de aportar cierta anonimidad a sus usuarios, lo cual, puede generar comportamientos ilícitos en ciertos casos. Recordar que la anonimidad no tiene lugar en redes blockchain privadas, pues en estas todos los participantes están identificados.

En lo referente a la **causa** los artículos 1275, 1276 y 1277 del Código Civil establecen que ésta ha de ser lícita, veraz y existente. Los contratos legales no serían capaces de asegurar la licitud, sin embargo, en el artículo 1277 CC se establece que la licitud y existencia de la causa se presume, por tanto no habría que expresarla en el contrato. Con la causa se haría referencia a la consciencia de las partes de que si se dan ciertas condiciones pactadas, se producirá la ejecución automática de sus consecuencias, por ello, las partes han de ser en todo momento conscientes de la naturaleza de las condiciones de ejecución.

Acerca del **consentimiento**, entendido este como el concurso entre la oferta y la aceptación sobre el objeto y la causa del contrato, en los contratos inteligentes, al ser contratos automáticos es de aplicación el párrafo tercero del artículo 1262 del Código Civil, de manera que el consentimiento quedará acreditado desde que se manifieste la aceptación. Así, en el momento en que se comiencen a llevar a cabo actuaciones que hagan indicar que la voluntad es la de someterse al contrato, la aceptación se consideraría dada y por consiguiente, el consentimiento también. Dicha aceptación tiene que ser confirmada por el oferente (art. 28 LSSICE).

En el ámbito de la contratación con consumidores, al tener estos un régimen de protección especial, se requiere un deber de información superior y tanto la oferta, como la información pre-contractual, como el contrato deberán darse en un soporte duradero y de forma que un consumidor medio pueda entender. (arts. 60, 97 y 98 del Texto Refundido de la Ley de Defensa de Consumidores y Usuarios) De ello se desprende que en contratos inteligentes con consumidores deberá traducirse el código a un lenguaje común entendible por un consumidor medio.

Surgen problemas en cuanto a la capacidad de obrar de las partes, pues hay que recordar que para que el consentimiento sea válido las partes han de tener capacidad de obrar,

conforme al art. 1263 CC. Tal y como se ha comentado, las blockchain públicas permiten cierta anonimidad, pues los sujetos actúan en ella a través de billeteras con claves que son públicas pero dichas claves públicas no siempre tienen fácil identificación con la persona física que está detrás de esta. Este problema se resolvería alojando el Smart contract en una red blockchain privada, puesto que en una red de este tipo sí que están identificados todos y cada uno de los participantes, de manera que cada clave está correctamente identificada con una identidad real, identidad que quedaría acreditada mediante el empleo de la firma electrónica utilizándola para firmar electrónicamente el contrato⁵².

2.2. IMPLICACIONES JURÍDICAS DE LAS CARACTERÍSTICAS DE LA TECNOLOGÍA BLOCKCHAIN:

A. Protección de datos personales: derecho al olvido

La Unión Europea, con la finalidad de promover una protección de los datos personales homogénea en todo el conjunto de la Unión, elaboró un Reglamento⁵³ para sustituir a la Directiva 95/46/CE. Esto debido a que con la Directiva, cada país trasponía a su ordenamiento las estipulaciones contenidas en ella de formas diferentes entre países, de manera que existían diferencias entre países en cuanto al régimen de protección de datos. Es por ello que puso en marcha el Reglamento General de Protección de Datos (RGPD en adelante), el cual es de directa aplicación y cualquier norma que lo contradiga no es válida.

El RGPD, definió a los datos personales como toda aquella información sobre una persona física que identifique o haga identificable a la misma. De esta definición se obtiene que el Reglamento únicamente se aplicará a la protección de datos de personas físicas, no jurídicas, y, además, se indica que cualquier dato que pueda identificar, directa o indirectamente a una persona, será dato personal, esto es, aquí se incluirían números de teléfono, datos de localización o los identificadores en línea (dirección IP) entre otros.

⁵² FETSYAK, I. “Contratos inteligentes... *cit.* p.212-216

⁵³ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

En el Reglamento se diferencian dos sujetos a los que será aplicable el mismo. Por un lado se dan los responsables del tratamiento de datos, los cuales, son aquellas personas físicas o jurídicas que deciden los fines para los que van a ser utilizados los datos. Por otro lado, tenemos a los encargados del tratamiento de datos, los cuales, tratan datos personales por cuenta del responsable pero sin tomar ellos decisiones sobre los mismos.

a) Problema

El problema que presenta la tecnología blockchain es que, en las redes públicas, al tener todos sus datos distribuidos públicamente en una red de ordenadores de manera descentralizada sin ningún nodo central que tome decisiones en cuanto a estos datos, se hace muy difícil la identificación del responsable de tratamiento de una base de datos de este tipo. Aquí es donde se halla el primer conflicto de la tecnología blockchain con el Reglamento de Protección de Datos Personales: la característica de la descentralización hace inaplicable el Reglamento a un sujeto concreto y por lo tanto no sería aplicable en este tipo de tecnología. En este sentido, la Agencia Española de Protección de Datos indicó en un artículo de prensa en noviembre de 2020⁵⁴ que una red blockchain como Bitcoin no constituiría un tratamiento de datos específico, pues esta se trata de una red con reglas definidas y preestablecidas *ad hoc* en su libro blanco (documento donde se explica el funcionamiento del algoritmo de Bitcoin) publicado en 2009, de manera que son los participantes de la red los que por decisión de ellos mismos deciden someterse a las características de la red.

Lo mencionado anteriormente hace referencia a las redes blockchain públicas, sin embargo, cuando se trate de redes blockchain privadas, sí que existe uno o varios nodos centrales que tienen control sobre quien puede ser participante de la red. Por tanto, en este caso sí que se da un responsable o encargado de tratamiento de datos a los que les será de aplicación el RGPD cuando traten datos personales de personas físicas.

Ahora bien, a pesar de que se trate de una red blockchain privada, surge otro problema en relación con la característica de la inmutabilidad. Como ya se ha mencionado en varias ocasiones a lo largo de este trabajo, los datos introducidos en una red blockchain no se pueden modificar ni eliminar una vez los bloques en los que se alojan son validados. Esto presenta un problema con derecho al olvido que aparece en el artículo 17 del RGPD, el cual establece que el responsable del tratamiento deberá suprimir los

⁵⁴ Agencia Española de Protección de Datos: *Blockchain (II): Conceptos básicos desde la protección de datos*. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos> (Consulta: 18 mayo 2022)

datos personales del interesado cuando éste lo solicite si se dan una serie de supuestos como que los datos personales ya no sean necesarios para los fines para los que se recogieron, que el interesado retire su consentimiento, que los datos recogidos deban suprimirse para cumplir con alguna obligación legal o que los datos hayan sido tratados de forma ilícita, entre otros.

b) Solución

Son varias las soluciones propuestas a este problema. Una de ellas es la que propone la abogada SARA ESCLAPÉS, en su exposición sobre blockchain y sus principales aspectos jurídicos⁵⁵. Dicha solución es la anonimización del dato introducido en la cadena de bloques. En este proceso lo que hará el responsable de tratamiento (nodo central en una blockchain privada) será, en primer lugar, guardar los datos en una base de datos externa a la blockchain encriptada con una función hash (secuencia alfanumérica) y en segundo lugar volcar a la blockchain únicamente el hash que descripta a la base de datos externa a la blockchain. De esta manera, cuando el interesado solicite la supresión de sus datos personales por uno de los motivos señalados en el artículo 17 del RGPD, el responsable del tratamiento borrará los datos de esa base de datos externa de manera que lo único que seguirá en la blockchain será una función hash que descripta una base de datos vacía y por tanto anónima. Lo mismo si se quiere la modificación, en este caso, se modificarán los datos de la base de datos externa y con el hash inicial se podrán seguir consultando los nuevos datos modificados.

⁵⁵ ESCLAPÉS, SARA. “Blockchain y sus principales aspectos jurídicos”. Minuto 14-20. Disponible en formato video en: https://www.youtube.com/watch?v=b98t_bPEqGc&t=634s&ab_channel=Autentia (Consulta: 18 de marzo de 2022)

3. CONCLUSIONES

Hoy en día la sociedad está viviendo un proceso de digitalización sin precedentes. La mayoría de las actividades y procesos ya son digitales. Motivos como el aumento de eficiencia, la reducción de personal o de burocracia explican que estemos viviendo este proceso de digitalización.

A lo largo de este trabajo se ha visto como la tecnología blockchain tiene características que permiten que la información compartida a través de la misma sea confiable, transparente e inmutable. Gracias a ello, las posibilidades de uso de esta tecnología son muy variadas y, en muchos casos, desconocidas, ya que todavía no se sabe con exactitud el potencial real que puede llegar a alcanzar.

Muchos de los ámbitos en los que opera esta tecnología han sido nombrados en este trabajo y se ha realizado un análisis de sus aspectos jurídicos, principalmente, de aquellos con mayor contenido económico. Básicamente se han tratado y explicado los aspectos jurídicos de tres ámbitos: los criptoactivos, los contratos inteligentes y la problemática con la protección de datos.

En el ámbito de la prestación de servicios de pago y de la prestación de servicios financieros, resultado de ese proceso de digitalización que se nombra en el comienzo de este apartado, son numerosas las innovaciones que están surgiendo. La tecnología blockchain, con el nacimiento y la expansión de los **criptoactivos** a partir de la misma es una de esas innovaciones.

Las posibilidades que ofrece la tecnología blockchain con sus características a los criptoactivos puede potencialmente mejorar la eficiencia del sistema financiero, principalmente gracias a la eliminación de intermediarios que ocasionaría unos menores costes de transacción, mejorar transparencia tanto en las prestaciones de servicios financieros como en la prestación de servicios de pago, así como aumentar la competencia entre los distintos actores participantes en los sistemas financieros, lo cual mejoraría las condiciones para las personas y evitaría abusos de autoridades centrales.

Sin embargo, todavía no existe una regulación uniforme en torno a los criptoactivos, lo que hace que todavía no exista seguridad jurídica y confianza en torno a los mismos lo que ocasiona que se den numerosos riesgos en la economía surgida a partir de estos

nuevos tipos de activos, ya que, al no tener naturaleza jurídica definida, la principal utilidad que se les están dando son la de productos de inversión.

En los criptoactivos sin respaldo (como *bitcoin* y *ether*), su valor únicamente depende de lo que los compradores y los vendedores crean que va a valer en transacciones futuras, por lo que, ante cualquier variación en el sentimiento general del mercado se producen fuertes variaciones en ese valor. Es por ello que este tipo de criptoactivos están sujetos a una fuerte volatilidad que, entre otras cosas, no les permite convertirse en medio de pago y que origina unos elevados riesgos de mercado y de liquidez para los inversores, sobretodo a los inversores minoristas.

Otro tipo de riesgos que conlleva la inversión en los criptoactivos son los riesgos de fraude o los riesgos operacionales. Estos tipos de riesgos son consecuencia de las características de la propia tecnología subyacente. Consecuencia de la anonimidad que pueden facilitar el riesgo de fraude es considerable, ya sea porque se puede utilizar blanqueo de capitales, para la creación y difusión de estafas piramidales, etc. Por otro lado, como riesgos operacionales, encontramos al originado por el hecho de que al no existir ninguna autoridad central, los usuarios son únicos responsables de sus criptoactivos, por lo que, si se da el caso de que pierden o se olvidan de las claves de acceso a sus billeteras digitales, no hay nadie a quien reclamar.

En definitiva, tal y como se ha visto en este trabajo, la normativa actual en este ámbito es escasa o nula para todos los riesgos existentes. En España, apenas existen obligaciones de la CNMV para una adecuada publicidad para la inversión en criptoactivos.

Para que se puedan aprovechar los beneficios que aporta esta tecnología minimizando los riesgos, es necesario una regulación que aumente la confianza y seguridad jurídica en torno a los criptoactivos. En este camino va la Propuesta de la Ley sobre Mercados de Criptoactivos (Ley MiCA), que busca armonizar un marco regulatorio a nivel europeo en este ámbito.

En el ámbito de los **contratos inteligentes**, en primer lugar, hay que destacar que este tipo de contratos autoejecutables deben hacerse en ámbitos en los que se den cláusulas cuyo cumplimiento se base en causas objetivas (seguros, préstamos, cadenas de suministro, certificados de calidad, acreditación de un título para acceder a empleo público, etcétera), es decir, dichos contratos no pueden hacerse en ámbitos de

contratación en los que la interpretación subjetiva entre en juego. No cabe duda de que el empleo adecuado de este tipo de contratación puede aligerar notoriamente la tarea de jueces y abogados, quienes a su vez, tendrán que adaptarse a estas innovaciones.

Destacar también que uno de los factores cruciales para que este tipo de contratos sigan adelante, es la importancia de unos buenos oráculos que les aporten información lo más real posible de los eventos ocurridos en el mundo físico, algo que es vital para evitar que cláusulas de estos contratos se autoejecuten equivocadamente. En mi opinión los retos jurídicos en este ámbito se encuentran aquí, es decir, en dotar de un marco normativo a los oráculos para evitar fraudes en la información.

En cuanto a su posible adecuación como contratos con efectos jurídicos se ha visto que estos pueden cumplir con los requisitos de validez para producir efectos jurídicos. Desde el punto de vista formal, el hecho de que estén redactados en fragmentos o piezas de código informático no es ningún problema para su validez formal, pues en el ordenamiento español impera el principio de libertad de forma. Desde el punto de vista material, los Smart contracts deberán contar con los requisitos de validez (consentimiento, objeto lícito y causa).

Sin embargo, dadas las características intrínsecas de determinados tipos de redes blockchain, como son las redes blockchain públicas, se presentan problemas en torno a la licitud del objeto y en torno a la capacidad de obrar para otorgar el consentimiento. Ambos problemas se originan porque, estos tipos de redes, tal y como se ha explicado, permiten cierta anonimidad a sus usuarios lo cual conlleva que bien se puedan llevar a cabo actuaciones fraudulentas, que harían que el objeto no fuese lícito, o bien no se permita determinar si el sujeto contratante tiene capacidad de obrar para dar validez a su consentimiento.

La anonimidad quedará eliminada en una red blockchain privada, por lo que, en conclusión, para que un Smart contract pueda alcanzar una validez jurídica adecuada, tiene que estar alojado en una red blockchain privada. Así, parece que en las redes públicas no sería posible que estos contratos produzcan efectos jurídicos con la regulación actual, sin perjuicio de que dicho Smart contract se pueda tomar como prueba en un procedimiento judicial en el que se quiera demostrar la existencia de una relación jurídica.

Como reto jurídico pendiente, quedaría el buscar fórmulas para identificar a los contratantes en un Smart contract alojado en una red blockchain pública, algo que ya se está intentando solucionar al obligar a todos los proveedores de criptoactivos y a los proveedores de custodia de los mismos a registrarse y a que identifiquen éstos a todos y cada uno de sus usuarios, tal y como se desprende de la Directiva 2018/843.

Finalmente, en cuanto a la **problemática para la protección de datos personales** que la tecnología blockchain presenta, se ha visto que en las redes blockchain públicas el Reglamento de Protección de Datos Personales no se puede aplicar, pues no hay ningún sujeto responsable de los datos. Por tanto, se considera que la participación en estas redes es voluntaria aceptando unas condiciones que han sido previamente informadas. En las redes privadas sí que existen responsables identificables del tratamiento de los datos por lo que en ellas sí que sería de aplicación.

Así, solo en las redes privadas se podría solucionar el problema que origina la inmutabilidad de la información y su conflicto con el derecho al olvido. La solución sería, como se ha explicado la anonimización del dato mediante el uso de una base de datos externa a la blockchain.

Como vemos, tanto para los problemas de la validez de los Smart contracts, como para los problemas con la protección de datos personales, la solución es el uso de redes blockchain privadas, algo que desnaturaliza el fin por el que surgió la tecnología blockchain, el cual es la descentralización y la eliminación de cualquier autoridad central. Sin embargo, tal y como se ha visto en este trabajo, la descentralización total no puede tener lugar con la normativa actual.

4. BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Blockchain (II): Conceptos básicos desde la protección de datos*. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos>

BANCO DE ESPAÑA «Especial. Criptoactivos» *Informe de estabilidad financiera. Primavera 2022*, p. 149-175.

BANCO DE ESPAÑA: Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Disponible en: [Banco de España - Servicios - De interés general - Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos \(bde.es\)](https://www.bde.es/banco-de-espana-servicios-de-interes-general-registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos)

BANCO SANTANDER: Guía para saber que son las criptomonedas. Disponible en: <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>

BBVA Openmind: Tecnología Blockchain y gestión de la cadena de suministro. Disponible en: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/tecnologia-blockchain-y-gestion-de-cadena-de-suministro/>

BBVA Research: *Smart Contracts: ¿lo último en automatización de la confianza?*. Disponible en (link para descargar pdf): <https://www.bbva.com/es/smart-contracts-contratos-basados-blockchain/>.

BIT2ME Academy: *¿Qué son los oráculos blockchain?*. Disponible en: <https://academy.bit2me.com/que-es-oraculos-blockchain/>

CHAMORRO DOMÍNGUEZ, M^a DE LA CONCEPCIÓN, «Aspectos jurídicos de las criptomonedas». Disponible en: <https://blockchainintelligence.es/wp-content/uploads/2019/04/Art%C3%ADculo-doctrinal-Aspectos-jur%C3%ADficos-de-las-criptomonedas-por-M-de-la-Concepci%C3%B3n-Chamorro-Rodr%C3%ADguez.pdf>

CNMV: Comunicado conjunto de la CNMV y del Banco de España sobre “criptomonedas” y “ofertas iniciales de criptomonedas” (ICOs) de fecha 8 febrero 2018. Disponible en:

https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07.pdf

CNMV: Consideraciones de la CNMV sobre “criptomonedas” e “ICOs” dirigidas a los profesionales del sector financiero de 8 de febrero de 2018 . Disponible en: <http://www.cnmv.es/Portal/verDoc.axd?t=%7b9c76eef8-839a-4c19-937f-cfde6443e4bc%7d>

CNMV: Nueva Circular de la CNMV de publicidad sobre criptoactivos presentados como objeto de inversión. *Nota de prensa*, 21 de enero de 2022. Disponible en: <https://www.cnmv.es/portal/verDoc.axd?t={67a4f7e8-49b7-42ec-8328-f8f4b2004cd8}>

CNMV: Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión de fecha 9 febrero de 2021. Disponible en: <https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D>

DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V0590-18 de 1 de marzo de 2018. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/>

DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V1149-18 de 8 de mayo de 2018. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/>

DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V2679-21 de 5 de noviembre de 2021. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/>

DIRECCIÓN GENERAL DE TRIBUTOS, Doctrina Tributaria, Consultas. Consulta V0486-22 de 10 de marzo de 2022. Disponible en: <https://petete.tributos.hacienda.gob.es/consultas/>

ENDESA: Se requieren unos 40kWh semanales para que compense el minado de bitcoin. Disponible en: <https://www.endesa.com/es/blog/blog-de-endesa/luz/cuanta-electricidad-gasta-minar-bitcoins>

ESCLAPÉS, SARA. “Blockchain y sus principales aspectos jurídicos”. Minuto 14-20. Disponible en formato video en: https://www.youtube.com/watch?v=b98t_bPEqGc&t=634s&ab_channel=Autentia

FETSYAK, I. “Contratos inteligentes: análisis jurídico desde el marco legal español”, REDUR 18, diciembre 2020, págs. 197-236.

FUENMAYOR, CARLOS «Criptoactivos: un nuevo activo de inversión» en *Instituto de Estudios Financieros*.

GOMA LANZÓN, IGNACIO., «¿Se puede constituir una sociedad con bitcoins?» Blog de Hay Derecho, de 9 de junio de 2014. Disponible en: <https://www.hayderecho.com/2014/06/09/se-puede-constituir-una-sociedad-con-bitcoins/>

IBM: Visión General de Blockchain. Disponible en: <https://www.ibm.com/es-es/topics/what-is-blockchain>

LIBRO BLANCO DE BITCOIN. Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

MENA ROA, MÓNICA, «La adopción de las criptomonedas en el mundo», de 15 de febrero de 2022 en Statista. Disponible en: <https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/>

MICROSOFT: Datos no relacionales y NoSQL. Disponible en: <https://docs.microsoft.com/es-es/azure/architecture/data-guide/big-data/non-relational-data>

PORXAS, N. y CONEJERO, M., “Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados” *Actualidad Jurídica Uría Menéndez* nº48 año 2018 p 24-36.

RAE: Definición de tecnología. Disponible en: <https://dle.rae.es/tecnolog%C3%ADa?m=form>

SUAREZ PUGA, ERNESTO ALEJANDRO., «Naturaleza y régimen jurídico de las criptomonedas. », *InDret* 2.2021, p. 383-396.

TERSTIEGE ORTIZ, MANUEL. «Aspectos jurídicos a tener en cuenta en la emisión de criptoactivos por la empresa (utility token vs security token)» *DPO&it law*, 26 de octubre de 2021.

TJUE: Sentencia del Tribunal de Justicia (Sala Quinta) de 22 de octubre de 2015. Asunto C-264/14. Base de datos: Curia. Disponible en: <https://curia.europa.eu/juris/liste.jsf?td=ALL&language=es&jur=C,T,F&num=C-264/14>

TRADINGVIEW. Capitalización total del mercado de las criptomonedas. Disponible en TradingView,

<https://es.tradingview.com/chart/Njjs7Wrv/?symbol=BITSTAMP%3ABTCUSD>

TS: Sentencia del Tribunal Supremo 326/2019, 20 de Junio de 2019. Base de datos: vLex. Disponible en: <https://vlex.es/vid/797938401>