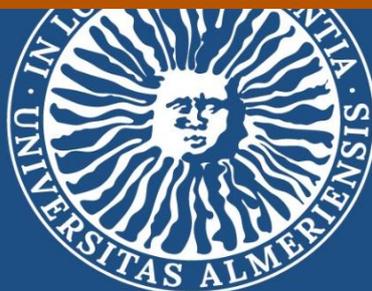


**25**  
1993 | 2018 **AÑOS**



**UNIVERSIDAD  
DE ALMERÍA**

# BLOCKCHAIN: LA TECNOLOGÍA QUE PUEDE CAMBIARLO TODO

Resumen

En este trabajo, veremos que es la <<blockchain>> y en qué medidas puede afectar esta tecnología en el mundo jurídico

# BLOCKHAIN: THE TECHNOLOGY THAT COULD CHANGE EVERYTHING

Summary

In this thesis, we will explore what <<blockchain>> is and in what ways this technology could affect in the legal world

Titulación cursada por el alumno: Grado en Derecho

Fecha/Convocatoria de defensa: Junio 2018

Autor: Jose Alejandro González Lores

Director: Ramón Herrera de las Heras

## ÍNDICE

1. Introducción.....	3
2. ¿Qué es la <<blockchain>>? Aplicaciones jurídicas.....	4
3. ¿Es compatible la <<blockchain>> con el derecho al olvido?.....	7
3.1 La protección de datos .....	7
3.2 Principios y derechos .....	8
3.2.1 Principios .....	8
3.2.2 Derechos .....	8
3.3 El derecho al olvido .....	9
3.3.1 El derecho al olvido en el ciberespacio .....	10
3.3.2 Derecho al olvido vs <<blockchain>>.....	11
4. <<Smart Contracts>> .....	13
4.1 ¿Qué son los <<smartcontracts>>? .....	13
4.2 Contratos tradicionales vs contratos inteligentes .....	14
4.3 Función multifirma en contratos inteligentes.....	15
4.4 Dobles depósitos en los contratos inteligentes .....	15
4.5 Aplicaciones que se le pueden dar a estos contratos inteligentes .....	16
4.6 Beneficios de los contratos inteligentes .....	17
4.7 Problemas que surgen con la creación de los <<smartcontracts>>.....	18
4.8 Validez legal de los <<smartcontracts>> en el sistema jurídico español... 19	
4.8.1 Los elementos de los contratos .....	19
4.8.2 Flexibilidad de los contratos .....	19
4.8.3 Jurisdicción y norma aplicable .....	20
5. El <<bitcoin>> .....	21
5.1 <<Criptomonedas o criptomonedas>> .....	21
5.2 ¿Qué es el <<bitcoin>>? .....	21
5.3 Problemas que surgen con el <<bitcoin>>.....	22
5.3.1 Desestabilización del sistema financiero centralizado.....	22
5.3.2 Competencia frente al sistema bancario tradicional .....	23
5.3.3 Transacciones ilícitas .....	23
5.4 Naturaleza jurídica del <<bitcoin>> .....	23
5.4.1 Títulos valores emitidos en soporte electrónico .....	24
5.4.2 El <<bitcoin>> como bien mueble incorpóreo.....	25
5.4.3 El <<bitcoin>>: Divisa virtual de flujo bidireccional.....	26
5.5 Marco legislativo.....	27
5.6 El <<bitcoin>> en el proceso penal .....	28
5.6.1 ¿Cómo relacionar el <<bitcoin>> a su titular? .....	28
5.6.2 El registro remoto en los equipos informáticos .....	28
5.6.3 Registro de almacenamiento masivo de información .....	29
6. Eficacia probatoria de la <<Blockchain>>.....	30
6.1 Valor jurídico del sellado de tiempo. Clases de sellos de tiempo .....	30
6.2 Actividad probatoria.....	31
6.3 Utilizando la <<blockchain>> como registro de la propiedad intelectual .....	31
6.4 <<Blockchain>> en el ámbito sucesorio.....	32

7. Reflexiones finales .....	33
8. Bibliografía.....	34

## 1. Introducción

El derecho es una de las materias de estudio más antiguas que existen, pero esto no quita que, a lo largo de los años, ha ido evolucionando y adaptándose a las realidades de su tiempo. El caso que estudiaremos a lo largo de este trabajo, es una nueva tecnología que ha surgido en los años anteriores, y que poco a poco, va tomando más relevancia en nuestra vida cotidiana: la tecnología de la cadena de bloques o en su terminología anglosajona <<blockchain>>. Debido a que cada vez más, esta tecnología se utiliza en ámbitos que están relacionados con el derecho, es necesario un estudio detallado, para poder incorporar esta realidad a nuestra legislación.

Esta tecnología es importante debido a que en un mundo cada vez más interconectado a través de la red, es necesario de medios o mecanismos que nos den una seguridad de que nuestras acciones quedan registradas de una manera legal, y que estas no podrán ser alteradas por ninguna persona, dándonos así un respaldo de fiabilidad.

Esta es la finalidad por la que nace la <<blockchain>>, un sistema informático en el que quedan constancia de forma segura todas nuestras acciones de manera inmutable, y esto es por lo que el derecho tiene que incorporarla dentro de sí, ya que es una realidad que cada vez más y más gente utiliza debido a los beneficios que aporta.

Por esto en primer lugar, hablaremos de que es la <<blockchain>>, cuando surgió y cuáles son los ámbitos jurídicos que puede afectar, es decir, una pequeña introducción a la materia.

Seguidamente, trataremos el tema relacionado con el derecho al olvido, ya que al ser una tecnología inmutable y pública se confrontará contra uno de los derechos constitucionalmente protegidos el derecho a la intimidad.

Como tercer punto a desarrollar será el relacionado con los <<smartcontracts>> o contratos inteligentes, en los cuales esta tecnología puede ser una gran innovación y cambiar por completo los contratos tal y como los conocemos actualmente.

A continuación, hablaríamos del <<bitcoin>> la <<criptodivisa>> por excelencia y que nació junto con la tecnología objeto de nuestro estudio. Esta <<cibermoneda>> actualmente se encuentra en su máximo esplendor y cada vez más especialistas la consideran como la próxima moneda universal desembarcando a las tradicionales divisas.

Finalmente, veremos cómo esta tecnología puede tener un efecto probatorio de que distintas transacciones se realizaron en un día y hora determinada sin la necesidad de ningún intermediario.

## 2. ¿Qué es la <<blockchain>>? Aplicaciones Jurídicas

<<Blockchain>> es un término que proviene de la lengua inglesa, cuyo significado es Cadena de Bloques. Este sistema surgió como un actor secundario cuando apareció la <<criptomoneda Bitcoin>>, pero muchos expertos ya comienzan a pensar que la <<Blockchain>>, es el actor principal por delante de la citada <<criptomoneda>>, puesto que son muy variadas las aplicaciones que tiene este procedimiento fuera del ámbito financiero. La <<Blockchain>> es una innovadora tecnología que es creada con la finalidad de proporcionar de propiedad digital a las personas que se encuentran en el mundo online evitando así depender de cualquier tipo de intermediario o autoridad central para controlar a los usuarios que participan en cualquier tipo de transacción, sino que está sería compartida con un gran número de nodos independientes entre sí que la adscriben y verifican sin necesidad de que haya confianza entre ellos.<sup>1</sup>

Lo que se graba en la <<blockchain>>, nunca podrá ser removido, quedando siempre constante, debido a que la cadena de bloques es un registro inmutable y permanente. Estamos hablando de una base de datos en la cual solo es posible añadir, por lo tanto, no se podría alterar ni borrar nada de lo que ya estuviera inscrito, todo esto solo bajo consenso. Otra destacable facultad de este sistema es que, aunque la red se cayera, con que solamente uno de los nodos citados anteriormente siguiera en funcionamiento, este sistema seguiría funcionando, no como sucede en casos en lo que todo depende de un servidor central, en el que, si ese servidor central cae, todo lo dependiente dejaría de estar activo, un claro ejemplo de esto sería, Facebook.

La <<blockchain>> está constituida por una serie de elementos, los cuales son:

- Bloques
- Mineros
- Nodos

A continuación, lo explicaremos más detalladamente:

**Bloques:** Son un cúmulo de transacciones verificadas e información adicional que se han incluido en la <<Cadena de Bloques>>. Cada bloque que forma parte de la cadena (excepto el bloque original, que inicia la cadena) estaría formado por:

1. Un código alfanumérico que enlaza con el bloque anterior.
2. El paquete de transacciones que incluye (cuyo número viene determinado por diferentes factores)
3. Otro código alfanumérico que enlazará con el siguiente bloque.

Lo que intenta el bloque que se está creando es averiguar a través de cómputos el tercer punto descrito anteriormente. Un código que sigue unas reglas determinadas para conseguir validarse y solo puede deducirse comprobándolo reiteradamente sin parar esto es lo que comúnmente determinaríamos como <<hash>>.

Avanzando en el tema, explicaremos como se forman estos bloques.

**Mineros:** Son quienes deben encontrar el <<hash>> que hemos descrito anteriormente. Este se trata de fórmulas matemáticas que compendian en reducidos caracteres una elevada cantidad de información, no será posible la existencia de dos <<hash>> idénticos y estos no se pueden alterar. Cada bloque cuenta con un hash nuevo y con el hash del bloque inmediatamente anterior, como medida de seguridad.

**Nodos:** Un nodo, básicamente es, un ordenador o chip conectado a la red (específica para la utilidad que se le esté dando uso. Ej. Red Bitcoin) utilizando un software que guarda y comparte una copia actualizada en tiempo real de la cadena de bloques. Una vez que el

---

<sup>1</sup> ¿Qué es Blockchain o Cadena de Bloques?. Retrieved from <https://www.economiasimple.net/que-es-blockchain-o-cadena-de-bloques.html>

bloque es validado y se añade, este hecho se comunica al resto de nodos y se incluye a la copia que cada uno acumula.<sup>2</sup>

Por lo tanto, podríamos decir que la <<Blockchain>> o Cadena de Bloques, es una tecnología que tiene la potencia de cambiar nuestra forma de relacionarnos en el mundo digital. En palabras de Marc Andreessen, creador de Netscape y socio de uno de los fondos de capital de riesgo más importantes de Silicon Valley:

“Una cadena de bloques es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está “distribuido” o es compartido entre muchas partes diferentes.

Solo puede ser actualizado a partir del consenso de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada.”

Una vez explicado de la manera más simple posible que es la <<blockchain>>, nombraré algunos ejemplos en los que este sistema de verificación va a poder aplicarse a cuestiones jurídicas y tendrá una gran relevancia en el futuro-presente:

- “Pagos en el mundo real: una startup llamada TenX ha creado una tarjeta prepago que se puede recargar con distintas <<criptodivisas>> para luego pagar con ella en cualquier sitio como si esa tarjeta tuviera dinero convencional, sin importar si ese establecimiento acepta o no este tipo de monedas virtuales.
- Carsharing: la empresa EY, subsidiaria de Ernst & Young Global Ltd está desarrollando un sistema basado en la cadena de bloques que permite a empresas o grupos de personas acceder a un servicio para compartir coches de forma sencilla. El llamado Tesseract permitiría registrar quién es el propietario del vehículo, el usuario de ese vehículo y generar los costes basados en el seguro y otras transacciones en este tipo de servicios.
- Almacenamiento en la nube: Los servicios de almacenamiento en la nube como Dropbox o Google Drive son centralizados y al usarlos estás confiando en que un único proveedor “responda” por los datos que almacenas en él. Storj es una startup que está testeando en forma de beta un servicio que permite que esto se haga de forma distribuida utilizando una red basada en la <<Blockchain>> para aumentar la seguridad y hacer menos dependiente el servicio. Sus usuarios podrán además alquilar el espacio que no utilicen a otros, al igual que hace Airbnb con alojamientos.
- Identidad digital: los últimos y gigantescos fallos de seguridad y robos de datos han hecho que la gestión de nuestras identidades se convierta en un problema muy real. La cadena de bloques podría proporcionar un sistema único para lograr validar identidades de forma irrefutable, segura e inmutable. Hay muchas empresas desarrollando servicios en este ámbito, y todas ellas creen que aplicar la tecnología de la cadena de bloques para este propósito es una solución óptima.
- Servicio públicos y gubernamentales: otro de los ámbitos más interesantes de la aplicación de la cadena de bloques es en los servicios públicos que podrían presumir así de una transparencia absoluta. Las áreas de actividad son múltiples: desde la gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades hasta la gestión de identidades. De hecho, el robo masivo de datos en Equifax han hecho que algunos propongan la sustitución de los números de la seguridad social en Estados Unidos con un sistema basado en

---

<sup>2</sup> ¿Qué es la Cadena de Bloques (Blockchain)?. [Blog]. Retrieved from <https://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/>

la cadena de bloques. Hay iniciativas incluso para "descentralizar el gobierno", y Bitnation es una de esos proyectos que tratan de llamarnos convertírnos en "ciudadanos del mundo".

- Seguridad social y sanidad: aunque se podría englobar dentro de los servicios públicos mencionados, la sanidad pública podría sufrir una verdadera revolución con un sistema de cadena de bloques que sirviera para registrar todo tipo de historiales médicos y resolver uno de los problemas clásicos de la gestión de la sanidad.
- Gestión de autorías: aunque relacionado con lo mencionado para el mundo de la música, Ascribe es una plataforma que trata de ayudar a creadores y artistas a atribuirse la autoría de sus trabajos a través de la cadena de bloques. Hay otras muchas plataformas en este ámbito (Bitproof, Blockai, Stampery, por ejemplo) que entre otras cosas permiten generar tiendas en las que se puedan comprar trabajos originales de una forma segura y sencilla.
- Voto Electrónico: Como te podrías imaginar, el coste de crear papeletas, organizar toda la infraestructura necesaria para gestionar el voto y el posterior conteo, tiene un coste altísimo. Ya se han probado sistemas de voto electrónico, pero han sido incapaces de resistir ataques de hackers y de tener fallos a la hora de hacer el recuento con total precisión. La <<Blockchain>> puede solucionar esto ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, infalsificable (un hacker necesitaría más poder computacional que los 500 superordenadores más potentes combinados, 256 veces) a un coste prácticamente nulo y de acceso público. Este sistema podría acabar con la sombra de "pucherazo" que sobrevuela en toda elección, especialmente en países en los que la corrupción está a la orden del día.
- Registro de propiedades: el gobierno japonés ha iniciado un proyecto para unificar todo el registro de propiedades urbanas y rústicas con tecnología de cadena de bloques, lo que permitiría contar con una base de datos abierta en la que se pudieran consultar los datos de los 230 millones de fincas y 50 millones de edificios que se estima existen en el país asiático. En Dubái están planeando algo muy parecido.
- <<Smartcontracts>> o Contratos inteligentes: es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan el lastre de la interpretación al no ser verbal o escrito en los lenguajes que hablamos. Los <<smartcontracts>> se tratan de "scripts" (códigos informáticos) escritos con lenguajes de programación, siendo los términos del contrato puras sentencias y comandos en el código que lo forma."<sup>3</sup>

---

<sup>3</sup> Pastor, J. (2017). Qué es blockchain: la explicación definitiva para la tecnología más de moda. Retrieved from <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>

### 3. ¿Es compatible la <<blockchain>> con el derecho al olvido?

Antes de hablar directamente sobre la relación de la <<blockchain>> con el derecho al olvido, tendremos que hablar de donde proviene este derecho al olvido y porque existe esta confrontación con la cadena de bloques.

#### 3.1. La protección de datos

Cualquier persona en el transcurso de su vida, dispersa por diferentes medios (actos administrativos, denuncias, demandas, redes sociales...) su información personal, pero debido a los grandes avances tecnológicos con los que nos encontramos hoy, es posible concentrar esa información. Debido a todos estos avances, sería posible que una persona con las cualidades suficientes y los medios necesarios, utilizase esta información personal para interferir en nuestra vida.

Este problema, ya tiene solución en aquellas sociedades desarrolladas, que viene a englobar lo que denominaríamos la dignidad humana, y estaría recogido en estas sociedades en el “derecho que tiene cualquier persona”.

Esto vendría recogido por ejemplo en nuestra constitución, en el título primero, de los derechos y deberes fundamentales, en su artículo diez que dice así:

“1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.”<sup>4</sup>

Pero todo lo expuesto anteriormente, no tendría valor alguno si no se lleva a la práctica, creando normas que protejan y sirvan en favor de la persona<sup>5</sup>.

La libertad de los hombres y las mujeres, para que sea posible, debería protegerse, entre muchas otras cosas, su intimidad, la cual puede ser ofendida mediante información falsa sobre ellos que podría divulgarse a través de medios informáticos. Por estos motivos, se crean en las actuales legislaciones las leyes específicas de protección de datos.

Con el término <<protección de datos>>, la doctrina jurídica entiende que es una protección legal que las personas tienen respecto a cómo se tratan de manera automática sus datos personales.

Nosotros podríamos entender a esta <<protección de datos>> como el deber que se tiene para con los ciudadanos ante la utilización de sus datos personales por terceras partes sin autorización, que pueda afectar en el desarrollo de su vida personal.

Por ello, lo que se trata con esta protección de datos, es proteger a las personas ante la posible utilización inadecuada de sus datos, pero sobretudo esa protección en el ámbito de la informática y las comunicaciones.

Para que esta protección sea eficaz, esa recopilación de datos debería de poder identificar al individuo o incluso permitir que se conozcan nuevas características sobre él, que pertenezcan a la esfera de su intimidad.

Además, sería necesaria que se utilizara la información personal sin la autorización del perjudicado, o para distintas cuestiones de las que el individuo hubiese autorizado.

---

<sup>4</sup> Boletín oficial del Estado. (1978). Constitución española. [online] Available at: <https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229>

<sup>5</sup> Peces Barba, G.: Derechos Fundamentales, Guadiana de Publicaciones, SA. Madrid, 1976, pg.159.

### **3.2. Principios y derechos.**

A continuación, describiremos una lista sobre los principios y derechos que debería recoger cualquier legislación actual sobre Protección de datos.

#### **3.2.1. Principios**

En referencia a los principios hablaríamos de:

- **Pertenencia de datos:** En relación con el ámbito y la finalidad con los que se hayan obtenido.
- **Exactitud y actualización:** por el cual los datos tienen que reflejar de manera veraz la situación actual del individuo.
- **Consentimiento del interesado:** Para que puedan ser tratada la información personal, excepto que la ley disponga de otra cosa.

El ministro de justicia de España, en la presentación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, que fue derogada por la Ley Orgánica de Protección de Datos, hace una clasificación de los principios que deberíamos destacar:

- a) “Principios de carácter general de la Ley entre los que cita:
  1. El principio de proporcionalidad.
  2. El de vinculación al fin.
  3. El de exactitud.
  4. El de transparencia hacia los afectados.
  5. El secreto del responsable (que nos introduce el nuevo concepto de la confidencialidad)
- b) Principios singulares:
  1. Recogida, con la necesidad de informar al afectado del alcance.
  2. Tratamiento, con el consentimiento o con una Ley específica que permita recoger los datos, aunque no haya consentimiento.
  3. Cesión también con el consentimiento del interesado como principio y la libre revocabilidad del consentimiento para ceder los datos.
- c) Principios especiales: Que son aquellos que afectan a los llamados datos sensibles.”<sup>6</sup>

#### **3.2.2. Derechos**

Pero para que estos principios se puedan seguir, se necesitaría que se ejerciesen unos determinados derechos, por los cuales el individuo pueda obtener la protección de datos de la que se habla. Estos derechos son:

- **El derecho a la autodeterminación:** Este derecho se refiere a la potestad que tiene cada individuo a como se utilicen sus propios datos y a conocer, en su caso, a conocer la información pertinente que se encuentran en soportes informáticos o susceptibles de dicho tratamiento.
- **Los derechos de información y acceso:** Es el derecho que tendrá el titular para saber con qué propósito han sido obtenidos y registrados sus datos personales.

---

<sup>6</sup> Davara Rodriguez, M. (2015). Manual de Derecho informático (11th ed., p. 77 y ss.). Aranzadi.

- Los derechos de rectificación y cancelación: Es la posibilidad que tendría el interesado en el caso de que los datos que se tengan de él sean inexactos o cuando ya hayan dejado de ser necesarios para el fin por el cual se habían registrado.

El ejercicio de estos derechos es llevado a cabo a través del procedimiento <<habeas data>>, regulado en la ley 1266 de 2008, se trata de un derecho por el cual, cualquier persona puede conocer, actualizar y rectificar toda esa información que pueda relacionarlo con ella y que se guarde o almacene en centros de información.<sup>7</sup>

De todos los derechos anteriormente citados, destacaremos el último, el derecho de rectificación y cancelación, recogido en el artículo 16 de la Ley Orgánica de Protección de datos, que dice:

“El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.”<sup>8</sup>

ya que este es el relacionado con el derecho al olvido, que nos incumbe respecto a la <<blockchain>>, debido a que esta innovadora tecnología confluiría con este derecho al olvido, que no es ni más ni menos que el derecho de los interesados a que se rectifique o cancele o borren de internet, cuando estos ya no sean necesarios para los fines por los que se publicaron o se obtuvieron; o simplemente cuando sea esa la voluntad del titular de los datos y quiera revocar el uso de los datos en los caso previstos por la legislación sobre protección de datos.

### 3.3. El derecho al olvido

Podríamos decir que el derecho al olvido proviene de dos fuentes principalmente:

1. El caso contra Google España de 2014, el cual fue resuelto por el Tribunal de Justicia de la Unión Europea, en el que se exigió que se eliminaran determinados resultados de información de un ciudadano español<sup>9</sup>.
2. El nuevo Reglamento General de Protección de Datos de la Unión Europea, que entra en vigor el próximo 25 de mayo.

El derecho al olvido podríamos definirlo, como bien apunta María Álvarez Caro<sup>10</sup> como aquel derecho a equivocarse o que a una equivocación pasada no marque y determine la vida de un individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante.

Otra definición que nos propone la misma autora, es que se conoce como derecho al olvido, a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la Red. Este tipo de definición, sería más cercana a la desindexación de la información en buscadores de internet, más que al propio derecho al olvido.

Por eso podríamos diferenciar en dos tipos de solicitudes:

- Solicitudes destinadas a la eliminación de la información de su fuente original

<sup>7</sup> Davara, M.A.: <<Intimidad, informática y seguridad jurídica en España>>, Boletín de la Fundación para el Desarrollo Social de las Comunicaciones (128) FUDNESCO. Madrid, abril, 1992, pg. 14.

<sup>8</sup> Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (1999). Retrieved from <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>

<sup>9</sup>Sentencia contra el caso Google. (2014). Retrieved from <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&amp;pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=276332>

<sup>10</sup> Álvarez Caro, María, Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital, ED. Reus, 2015, España, pág.68.

- Solicitudes de desindexación de la información, dirigidas a los buscadores de internet.

La principal diferencia entre ambas solicitudes es que mientras que en una si se borra definitivamente la información, en la segunda, en la desindexación, no se borraría la información, lo que pasaría en estos casos es que, esas entradas que ofrecen los buscadores de internet con la información sensible, no se borrarían, sino que se ocultarían en dichos buscadores para que no pueden ser encontrados a través de su motor de búsqueda.

En relación con lo anterior, la mencionada sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, reconoce este derecho al olvido a través de una prerrogativa que tiene el individuo, para pedir que se bloqueen las entradas de los motores de búsqueda, en todos aquellos casos, en los que contengan información que le sea perjudicial, o en su caso sea obsoleta, errónea, falsa, incompleta o irrelevante.

Respecto, al Reglamento General de Protección de datos de la Unión Europea, el derecho al olvido tiene lógica como razón del derecho que tienen los ciudadanos a solicitar y promover que, los responsables de los datos propios que han sido publicados, sean borrados, cuando estos ya no tengan la función original por la que se recogieron, cuando se haya retirado el consentimiento a que estos sean expuestos o cuando se hayan obtenido de forma ilícita.<sup>11</sup>

### **3.3.1. El Derecho al olvido en el ciberespacio**

El derecho al olvido es una figura que ha adquirido mucha importancia en los tiempos cibernéticos actuales debido a que actualmente se puede adquirir y pasar grandes cantidades de información, pudiendo ser esta de carácter personal, lo que produciría grandes perjuicios a derechos fundamentales como el de la privacidad y la protección de datos.

Este derecho al olvido surge como una medida de protección ante tan incipientes ataques contra nuestro derecho de privacidad en la red. El ejercicio del derecho al olvido podría hacerse en ámbitos físicos y digitales, y dentro de esto destacamos dos aspectos: el técnico y el jurídico.

Por un lado, el aspecto técnico, se refiere a las peticiones que se harían de desindexación de la información relativa a los motores de búsqueda.

Por otro, respecto al aspecto jurídico, en el cual se ejercita el derecho de cancelación de los datos personales, en el cual no se borra la información de forma permanente, si no que se oculta.

Toda esta controversia nace debido a que este problema de la protección de datos en internet surge después de la inclusión en las constituciones y reglamentos europeos modernos, de los derechos humanos, por lo que estos no tienen ningún tipo de enfoque para esta nueva casuística que surgiría con posterioridad. Pero podríamos destacar una cosa, tanto los derechos humanos, como Internet, son derechos universales.

A pesar de esto, el derecho al olvido no es un derecho como tal, ya que hay cierto tipo de información que es de interés público y se ejecutará este derecho, se privaría de otros derechos como la libertad de expresión y el acceso a la información.

Hay dos características importantes de este derecho al olvido, la primera, es que la edad mínima que se establece en el Reglamento General de Protección de Datos de la Unión Europea es de 16 años como regla general, pero, sin embargo, esta edad podría bajarse

---

<sup>11</sup> Mendoza Enriquez, O. (2017). *Fodertics 6.0: Los nuevos retos del derecho ante la era digital*(1st ed., p. 370 y ss). Granada.

hasta los 13 años a libre elección de los estados miembro. Por lo que, si alguno de estos menores de edad, pero que fueran mayores de 16 años (o de 13, dependiendo del Estado miembro), podrían ejercitar este derecho al olvido, sin la necesidad de tutores legales. La segunda, a quienes se le aplica este es a los responsables y encargados del tratamiento de los datos de las empresas aquí, en la Unión Europea.

### 3.3.2. Derecho al olvido vs <<blockchain>>

Uno de los puntos fuertes de la <<blockchain>> es su inmutabilidad e inalterabilidad, ya que una vez que se añaden datos a la “cadena”, estos no podrán ser borrados. Por esto, a pesar de que el nuevo reglamento de protección de datos no ha entrado en vigor, ya podemos ver como la <<Blockchain>> estaría en un limbo jurídico. Últimamente, algunos expertos se encuentran preocupados por la idea de que la <<Blockchain>> se confronte con el derecho al olvido, presente en el reglamento anteriormente citado, el cual entrará en vigencia a partir del 25 de mayo del 2018. Este <<derecho al olvido>> trata, esencialmente, de la posibilidad de solicitar que se supriman los datos personales de los medios que los contengan si la persona lo desea<sup>12</sup>.

Según Gisela Santos, asociada senior de Garrigues: “La <<blockchain>> es una tecnología imparable. La clave para abordarlo pasa por encontrar un equilibrio entre tecnología y privacidad”<sup>13</sup>.

Por eso, llegados a este punto habría que hacerse una pregunta: ¿Qué pasaría si la información contenida en uno de esos bloques tiene almacenados datos personales y alguien quiere ejercitar ese derecho al olvido?

La respuesta a tal cuestión, en la situación actual en la que nos encontramos sería que esa tarea resultaría completamente imposible, no podría borrar esos datos, aunque solicitará ese derecho al olvido, regulado en el reglamento que entra en vigor el 25 de mayo de este año. Todo esto debido a que, como explica la firma consultora Kwori, los sistemas actualmente utilizados de <<Blockchain>>, incluso el borrado de datos quedaría registrado, lo que resultaría una bifurcación. Por lo que, aunque en la nueva cadena no existirían esos datos, en la vieja continuaría registrado, todo esto, sin mencionar toda la polémica que conlleva la bifurcación de la red.

Una opción que se baraja como solución al problema del que hablamos, sería borrar la llave privada correspondiente a la cuenta, lo que produciría en teoría, una inaccesibilidad a los datos que contiene. Pero claro, esto simplemente es la teoría, ya que, en la práctica, esa llave privada se podría llegar a recuperar mediante diferentes técnicas, incluyendo entre ellas la fuerza bruta (procedimiento criptográfico para recuperar una clave probando todas las combinaciones posibles).

Otra opción que propone la consultora Kwori para eliminar los datos en una <<blockchain>> y por lo tanto ejercer ese derecho al olvido legalmente establecido, sería crear un nuevo sistema de contabilidad distribuida que permita la edición por parte de unos administradores designados. Esta es una idea también compartida por Natalia Martos, socia de la firma legal Andersen Tax & Legal, quien dice que: “Se está trabajando en cadenas privada y también editables. En estas últimas, se permite que uno o varios

---

<sup>12</sup> Perez, I. (2017). BLOCKCHAIN Y DERECHO AL OLVIDO: ELIMINANDO DATOS DE LA CADENA. Retrieved from <https://www.criptonoticias.com/regulacion/blockchain-derecho-olvido-eliminando-datos-cadena/>

<sup>13</sup> Garcia Zarzalejos, A. (2017). Bruselas, tenemos un problema: el 'blockchain' choca con la normativa de datos. Retrieved from [https://www.elconfidencial.com/economia/2017-04-30/tecnologia-disruptiva-blockchain-cadena-bloques-derecho-al-olvido-reglamento-proteccion-datos\\_1363610/](https://www.elconfidencial.com/economia/2017-04-30/tecnologia-disruptiva-blockchain-cadena-bloques-derecho-al-olvido-reglamento-proteccion-datos_1363610/)

administradores puedan reescribir o cambiar bloques de información de posición en un tipo de <<blockchain>> editable que lo permita sin alterar la totalidad de la cadena”. Esta quizá sea la opción más admisible y la que puede llegar a utilizarse en un futuro no muy lejano.

Aparte, la citada consultora también ha apuntado que, en los sistemas de identidad, se puede producir un mal que afecte a los usuarios ya que no se podría corregir los datos falsos.

Pero podría existir otra solución a este conflicto, como la que encontramos en la Sentencia número 5129/2014, de 29 de diciembre, de la sala de lo Contencioso-administrativo, sección primera de la audiencia nacional resolvió que, pese a que es imposible eliminar o suprimir datos de su fuente de información, lo que sí se puede hacerse es eliminar de la lista de resultados de los buscadores ese vínculo entre el dato personal y la información contenida en ella. Es decir, pese a que lo que se encuentra almacenado en <<Blockchain>> es inalterable, se puede tratar de ocultar públicamente.

Sin embargo, por ahora no existe ningún tipo de idea para solucionar este problema que ha surgido con la <<blockchain>>, por lo que habría que esperar a la aplicación del reglamento para ver cómo se resuelve este conflicto y cuál es la respuesta del legislador.<sup>14</sup>

---

<sup>14</sup> Ros, E. (2018). Blockchain vs Derecho al olvido. Retrieved from <https://www.bonattipenal.com/blockchain-vs-derecho-al-olvido/>

## 4. <<Smartscontracts>>

### 4.1. ¿Qué son los smartscontrarcts?

Antes de comenzar a explicar que es un <<smartcontract>> recordaremos que es un contrato.

Nuestro código civil establece una regulación de contrato, pero no define lo que es. El contrato es enumerado entre las fuentes de las obligaciones, en el artículo 1089 del código civil; el artículo 1091 dice que “las obligaciones que nacen de los contratos tienen fuerza de ley entre las partes contratantes”, y el artículo 1254 expone “el contrato existe desde que una o varias personas consienten en obligarse, respecto de otra y otras, a dar alguna cosa o prestar algún servicio”<sup>15</sup>. Una vez analizados estos preceptos legales se podría entender que el contrato aparece por la conjunción de los consentimientos de dos o más personas con la finalidad de que surjan unas obligaciones recíprocas entre ellas.

Por lo tanto, podríamos entender el contrato convencional como un acuerdo entre dos o más partes, en el que se establece lo que se puede hacer, como se puede hacer, que pasa si se incumple... Es decir, las partes contratantes van a estar sometidos a unas reglas que ambos deben cumplir.

Hasta ahora los contratos han sido documentos verbales o documentos escritos, los cuales estaban sometidos a leyes y jurisdicciones territoriales, y usualmente eran necesario la presencia de notarios, lo que equivale a más costes y tiempo, por lo que no era accesible para todo tipo de personas. Pero este no es el mayor problema de los contratos convencionales, sino que la mayor cuestión que se plantea a estos es que, los contenidos de los contratos pueden estar sujetos a la interpretación.

Para solucionar estas controversias, surgieron los <<smartcontracts>> o contratos inteligentes, en su traducción al español, que, aunque parece algo novedoso, llevan desarrollándose desde 1993, año en el que el renombrado criptógrafo Nick Szabo definió el término por primera vez. El señor Szabo propuso este sistema en la década de los 90, sin embargo, la tecnología aún no estaba tan desarrollada para hacerlos factibles.<sup>16</sup>

Los <<smartcontracts>> podríamos definirlos como un código o protocolo informático que simplifica la convalidación y cumplimentación de un contrato automáticamente<sup>17</sup>. Estos están integrados en la cadena de bloques, en forma de <<scripts>> (códigos informáticos) y no necesitarían la intervención de nadie para comprobar y ejecutar su cumplimiento.

Al contrario que los contratos convencionales, un contrato inteligente tiene la capacidad para aplicarse por sí mismo, autónomamente y de manera automática, sin la necesidad de que haya ningún tipo de intermediario, como, por ejemplo, los notarios, evitando así la libre interpretación.

Por otro lado, los contratos inteligentes pueden ser creados tanto por personas físicas como por personas jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma (máquinas expendedoras). Estos tienen validez sin depender de ninguna autoridad, debido a que es un contrato público, ya que puede ser visible por todo el mundo y no se puede modificar debido a que está integrado en la <<Blockchain>>, la cual la dota de un carácter descentralizado, inmutable y transparente.

---

<sup>15</sup> Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. (1889). Retrieved from <https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763>

<sup>16</sup> Szabo, N (1 septiembre 1997). <<Formalizing and securing relationships on public networks>>. Peer-reviewed journal on the internet. Vol. 2, 9. <http://ojphi.org/ojs/index.php/fm/article/view/548/469>

<sup>17</sup> Christindis, K y Devetsikiotis, M. (10 de mayo, 2016). <<Blockchains and Smart contracts for the internet of things>>. Institute of electrical and electronic engineers. Vol. 4, pp. 2292-2303

Todo esto quiere decir que, cuando se da una condición que se ha programado en el <<script>>, el contrato ejecuta automáticamente la cláusula correspondiente.

Para hacerlo ver de una manera más clara, explicaremos un ejemplo sobre una casa de apuestas. Imaginemos que queremos apostar un montante de dinero X a que un equipo Y gana un partido. Se debería de crear una cuenta, en la que se establezca y quede registrada esa apuesta con la cantidad X apostada. Una vez finalizado el partido en cuestión, si el equipo Y resulta el vencedor, el contrato, automáticamente, accederá a la base de datos previamente establecida por la casa de apuestas y lo comprobará, y al verificar que es cumple la condición, enviará los fondos al vencedor de la apuesta.

Estos <<smartcontracts>> no son controlados por ninguna de las partes contratantes, se trata de un sistema descentralizado.<sup>18</sup>

Esto significa que:

1. “Se programan las condiciones.
2. Se firman por ambas partes implicadas.
3. Y se coloca en una <<blockchain>> para que no pueda modificarse.

Y, por otra parte, tienen como objetivo principal:

- Implementar un estado de seguridad mayor al del contrato tradicional.
- Reducir costes.
- Reducir el tiempo asociado a este tipo de interacciones.”<sup>19</sup>

Este tipo de contratos tienen un potencial impresionante, por eso deberíamos resaltar que, al encontrarse repartido por incontables ordenadores, se evita así que nadie los pueda privatizar, lo que conlleva la eliminación de la burocracia, que sean censurados y los grandes costes y tiempo que conllevaría el proceso convencional.

Decididamente, si aunamos los principios de los contratos inteligentes con la creatividad de los desarrolladores informáticos, el resultado podría ser asombroso, debido a la gran cantidad de posibilidades que se podrían crear, siendo accesibles para todo el mundo y con costes que podrían ser incluso gratuitos.

## **4.2. Contratos tradicionales vs contratos inteligentes**

En este apartado vamos a hablar de las mayores diferencias que podemos encontrar entre ambos contratos.

Los contratos en papel, son aquellos que están escritos en un lenguaje natural, es decir, puede ser redactado en cualquier idioma, pero que este sea entendible para los contratantes.

Una vez que las condiciones son aceptadas y es firmado, para que resulte válido se necesitaría de un notario.

El modo en el que se cumplen las obligaciones va a depender de la manera en que cada parte entienda correcta, puesto que, en un contrato, las cláusulas normalmente benefician a una parte en perjuicio de la otra.

Los <<smartcontracts>> se diferencian de lo anterior, intentado mejorar técnicamente, en:

El lenguaje no es natural, sino que es un lenguaje virtual, un lenguaje de programación informática. Al igual que cada programa de ordenador o cada aplicación móvil están

---

<sup>18</sup> Frías García, V. (24 de junio, 2016). Smart contracts, ¿el futuro del blockchain? [artículo de blog]. Recuperado de <http://www.intelygenz.es/smart-contracts-el-futuro-del-blockchain/>

<sup>19</sup> mi ethereum. (2018). SMART CONTRACTS O CONTRATOS INTELIGENTES. [online] Available at: <https://miethereum.com/smart-contracts/>

programados para realizar una serie de tareas, los contratos inteligentes también realizan tareas bajo unas instrucciones introducidas previamente.

Esto hace que en el modo de cumplimiento no haya diferentes puntos de vista, sino una única lectura: Si se da la condición establecida, el contrato ejecuta automáticamente la consecuencia a dicha acción.

La responsabilidad legal del contrato inteligente sigue en desarrollo. Lo que es indudable es que no requiere de un intermediario de confianza, reduciendo así los costes y el tiempo de las interacciones.

### **4.3. Función multifirma en contratos inteligentes**

Esta función, es una característica de los <<smartcontracts>>, por la cual, dos o más personas se deben de poner de acuerdo para hacer cumplir las condiciones de un contrato<sup>20</sup>. Para entenderlo mejor, expondremos un ejemplo clarificador:

Imaginemos que Pedro y María son dos amigos que quieren comprar un solar entre los dos.

Este tipo de compra, es de una gran cantidad de dinero por lo que tendrán que ir ahorrando, para lo que deciden hacer un contrato inteligente en el cual cada uno tiene que ingresar alrededor de 600 euros al mes hasta alcanzar los 50.000 euros que vale el solar. El contrato inteligente bloqueará esos fondos hasta que se cumplan las condiciones del contrato.

Una vez se llegue a la cantidad de 50.000€, uno de los dos podría sacar todo el dinero por su cuenta y eso sería un problema, pero para que algo así no suceda existe la función multifirma.

Ésta permite que todas las partes deba aprobar la acción para poder sacar el dinero en cuestión.

En este caso concreto, Ana no podría sacar el dinero sin que Luis esté de acuerdo, y viceversa. A través de la función multifirma son ambos los que tienen que estar de acuerdo, haciendo así que ninguno se pueda apoderar de la totalidad del dinero.

### **4.4. Dobles depósitos en los contratos inteligentes.**

En este apartado, nos encontramos ante otra característica de los contratos inteligentes, mediante la que se puede eliminar al intermediario del proceso.

Los dobles depósitos dan la posibilidad de que dos personas que no se conocen, por lo que no existe una confianza recíproca, puedan realizar una transacción igualmente segura para los dos a través del <<smartcontract>>.

Este tipo de contrato obliga a confiar en una dirección de la cadena de bloques un capital para el cumplimiento del contrato.

El acuerdo tiene duración limitada, por lo que, si no se cumple, el <<smartcontract>> redirigirá el dinero a otra dirección de la cadena de bloques de la que nadie podrá sacarlos nunca.

Esta cualidad fuerza a llevar a cabo lo acordado entre las partes actuantes, puesto que si no se cumplen, los fondos desaparecerían<sup>21</sup>.

Vamos a ver esta característica de una forma práctica, para que sea más entendible:

---

<sup>20</sup> Direcciones Bitcoin multifirma. [Blog]. Retrieved from <https://blog.bit2me.com/es/direcciones-bitcoin-multifirma/>

<sup>21</sup> ¿Qué son los contratos inteligentes o smart contracts? Bitcoin y Ethereum o el dinero programable. (2015). Retrieved from <https://www.royfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/>

Supongamos que Juan quiere comprar una pizza a domicilio a Pizzas Peperoni, y esta tiene un valor de 15€.

En el método tradicional habría dos formas, la primera que Juan pague la pizza en cuestión y que Pizzas Peperoni, no se la envíe o, que Pizzas Peperoni mande la comida antes de recibir el dinero y que Juan no le pague, en las dos situaciones hay una incertidumbre sobre si se recibirá el dinero o no.

Esto se solucionaría con un contrato inteligente de doble depósito, por el cual Juan pagaría 15€ para el contrato inteligente y otros 15 de depósito, mientras que Pizzas Peperoni pagaría 30€ pero solo como depósito de seguridad.

El <<smartcontract>> se ejecutará según las reglas establecidas por Juan y Pizzas Peperoni, por lo que se cumplirá si Juan recibe la pizza y Pizzas Peperoni los 15€, además al cumplirse el contrato, ambos recibirán su depósito de seguridad como compensación de haber hecho cumplir la seguridad del contrato.

Esto quiere decir que, en el caso de que una de las partes o ambas no cumplen con lo establecido, nadie obtendrá ninguna cantidad de dinero, lo perderán como penalización por incumplimiento de contrato.

Este tipo de doble depósito lo que persigue es que no se produzcan engaños y procura que los contratantes lleguen a acuerdos amistosos.

Este tipo de <<smartcontract>> ya es posible utilizar en mercados descentralizados como los portales Bithalo<sup>22</sup> y Blackhalo<sup>23</sup>.

#### **4.5. Aplicaciones que se le pueden dar a estos contratos inteligentes.**

Al tratarse los contratos inteligentes y la <<blockchain>> de tecnologías de nueva generación, los usos que hasta día de hoy se les están dando, no serán en nada comparables con los que se les den en un futuro.

A continuación, expondremos una serie de usos que ya se les están dando a estos contratos inteligentes en el mundo actual:

- “En el ámbito de los servicios financieros:
  - Préstamos: Cuando alguien solicite un préstamo y este no lo restituya en el tiempo establecido, se ejecutaría el contrato para retirarle las garantías.
  - Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente.
  - Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos.
  - Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso).
  - Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.
  - Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

---

<sup>22</sup> <http://bithalo.org/>

<sup>23</sup> <https://www.blackhalo.com/>

- Automatización de pagos y donaciones: se pueden acordar pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente lo que haría es verificar que se cumplen las reglas para realizar automáticamente la donación.
- En el ámbito de los servicios de la salud.
  - Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.
  - Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación.
  - Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT -Internet of Things- (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.
- En el ámbito de la propiedad intelectual.
  - Distribución de royalties: <<el smartcontract>> calcula y distribuye los pagos de royalties a artistas y otras partes asociadas según los términos acordados.
- En el ámbito de los servicios energéticos.
  - Estaciones autónomas de recarga para vehículos eléctricos: el contrato procesa un depósito, habilita la estación de recarga y devuelve los fondos restantes una vez completados.
- En el ámbito del sector público.
  - Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto a nivel de encuesta como a nivel estatal.
  - Apuestas: dos o más partes pueden apostar sin que se resienta su seguridad y sin necesidad de un tercero a través de un contrato inteligente que asegure unas condiciones concretas.
  - Propiedades inteligentes: una casa, un coche, una nevera, una lavadora... todos los objetos que se puedan conectar a Internet se consideran propiedades inteligentes (del inglés, smart property). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos o alquilarlos de forma automatizada.”<sup>24</sup>

#### **4.6. Beneficios de los contratos inteligentes.**

Una vez que ya sabemos de qué tratan y para que podrían ser utilizados estos <<smartcontracts>>, pasaremos a explicar cuáles son los beneficios de este tipo de contratos de la nueva era digital.

- Autonomía: En estos contratos no se necesitaría la intervención de un intermediario, por lo que no se necesitaría que alguien lo validase, como por ejemplo un notario.

---

<sup>24</sup> SMART CONTRACTS O CONTRATOS INTELIGENTES. Retrieved from <https://miethereum.com/smart-contracts/>

- Costes: En relación con el punto anterior, si se excluye a una tercera persona que lo valide, también se excluirán los costes que esa persona conlleva, lo que resultaría contratos con precios reducidos.
- Confianza: Al estar integrados, los <<smartcontracts>>, en la <<Blockchain,>> estos se incluirían directamente en la cadena de bloques, por lo que se encriptaría automáticamente, haciéndolo accesible solo a las personas contratantes, impidiendo que nadie ajeno al contrato pudiera modificarlo, ni una de las partes sin consentimiento de la otra, por lo que no se podría incurrir en estafa.
- Velocidad: Estos contratos serían mucho más veloces debido a que conforme se cumplan las condiciones establecidas en el, se producirían los resultados de forma automática.
- Seguridad: Al estar integrados en la <<Blockchain>>, estos quedan registrados de forma pública e inmutable.
- Nuevos modelos de negocio: Como hemos visto, al reducirse los costes con este tipo de contratos, se podrían crear nuevos negocios como el acceso automatizado a vehículos o contratos relacionados con el internet de las cosas.

#### **4.7. Problemas que surgen con la creación de los <<smartcontracts>>**

A pesar de todos los beneficios que acarrearán esta nueva modalidad de contrato, surgen muchas cuestiones que pueden producir problemática a la hora de la verdad como, por ejemplo:

- Aplicación en el "mundo real". Los <<smartcontracts>> son simplemente software y como tales se pueden "ejecutar", o mejor dicho pueden administrar el estado de los datos a los que tienen acceso en la cadena de bloques. Pero, más allá de eso, tienen poco alcance. Dentro del futuro previsible ningún tribunal podrá hacerlos cumplir y pocos estarán dispuestos a confiar únicamente en ellos para estructurar todos los términos de una transacción comercial.
- Flexibilidad. Los <<smartcontracts>> parecen dar por supuesto que las partes pueden determinar todos los aspectos de las negociaciones al inicio de su transacción. Pero en el mundo real, los contratos acaban a menudo por ser imprecisos, pues lo que sucede después de que las partes lleguen a un acuerdo con frecuencia es imprevisible. Los <<smartcontracts>> deben tener mecanismos que permitan a las partes modificar sus acuerdos cuando lo deseen mutuamente.
- Adopción. Las ventajas más importantes de la adopción de los <<smartcontracts>> se materializan cuando numerosas entidades empiezan a automatizar sus interacciones utilizando <<smartcontracts>> y un bloque de cadenas creado específicamente para la interacción entre varias partes. Dado que en la actualidad solo un número limitado de personas tienen conocimientos técnicos para desarrollar e implementar sistemas de <<smartcontracts>>, esto supone un verdadero reto.
- Responsabilidad legal. Los <<smartcontracts>> plantean un reto importante para las autoridades reguladoras, pues permiten la creación de versiones automatizadas descentralizadas de servicios P2P, como Uber o Airbnb, que conectan a las personas y manejan los pagos sin necesidad de una empresa intermediaria. Los reguladores se quedarían sin objetivo al que dirigirse porque detrás no hay entidad legal alguna.

## 4.8. Validez legal de los <<smartcontracts>> en el sistema jurídico español

### 4.8.1. Los elementos de los contratos

Debido a que los <<smartcontracts>> no son actualmente muy utilizados, puesto que no están perfeccionados al cien por cien, se nos plantean varias cuestiones desde el ámbito legal. El Sistema jurídico español, no los contempla aun, y tampoco tenemos constancia de jurisprudencia que puedan solventar nuestros problemas. Pero a la hora de establecer los requisitos mínimos exigibles a la hora de validar un contrato inteligente, habríamos de aceptar la normativa general de contratos, establecidos en el Título II, Capítulo segundo, de los requisitos esenciales para la validez de los contratos, en el artículo 1261, el cual dice: “No hay contrato sino cuando concurren los requisitos siguientes: 1.º Consentimiento de los contratantes. 2.º Objeto cierto que sea materia del contrato. 3.º Causa de la obligación que se establezca.” En referencia a este artículo también deberíamos de mencionar el artículo 23 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, el cual establece, en su apartado primero, párrafo primero: “Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez.”; ya que todo <<smartcontract>> sería realizado a través de una forma telemática.<sup>25</sup>

En relación con los elementos de los contratos en los <<smartcontracts>> (los cuales utilizan la tecnología <<blockchain>>), se nos puede presentar un grave problema, ya que sería de dificultosa identificación si la persona que está contratando se trata de un menor de edad o un incapacitado; o si se está comerciando con algún tipo de objeto ilícito.

### 4.8.2. Flexibilidad de los contratos

En los contratos tradicionales, es normal que sucedan errores a la hora de redactarlos. Por lo que en los contratos inteligentes no va a ser una excepción, pero aquí la subsanación de estos errores van a ser complejos, primero, porque al estar escrito en un lenguaje de programación, sería necesario que ese abogado estuviese familiarizado con ese lenguaje para ver donde se encuentra ese error o en su caso, el programador que quiera subsanar ese error debería ser abogado; y segundo, y por ello no menos importante, nos encontraríamos ante la situación en la que ese contrato ya se hallase inmerso en la cadena de bloques, por lo que sería inmutable.

Un claro ejemplo de esta situación sería el icónico caso de “The DAO”, la cual era una organización que operaba de forma descentralizada y autorregulada a través de varios contratos inteligentes. El funcionamiento de la DAO en términos generales era que <<cualquier persona del mundo podía dar su dinero a modo de capital social y automáticamente, el contrato le asignaría las participaciones que le correspondieran, cada miembro de la organización podría proponer en que gastarse el dinero y el <<smartcontract>> ejecutaba las acciones en base a los votos de todos los participantes>>.<sup>26</sup>

---

<sup>25</sup> Prenafeta Rodríguez, J., (15 septiembre, 2016). Smart contracts: aproximación al concepto y problemática legal básica [artículo de blog] Recuperado: <http://diarilolaley.laley.es>.

<sup>26</sup> Hernandez A., (03 octubre, 2016). Pronto firmarás contratos irrompibles que aseguran su propio cumplimiento. [artículo de blog]. Recuperado de [http://www.eldiario.es/hojaderouter/internet/contratos\\_inteligentes-smart\\_contracts-tecnología-blockchain-derecho\\_0\\_564494160.html](http://www.eldiario.es/hojaderouter/internet/contratos_inteligentes-smart_contracts-tecnología-blockchain-derecho_0_564494160.html).

Este sistema parece ideal, pero hemos de decir, que finalmente en el código había una vulnerabilidad, que un miembro supo explotar para así hacerse con una suma de <<criptomonedas>> valoradas en unos 45 millones de euros.

Además de los errores que se pueden presentar a la hora de redactar un contrato, lo más complicado de ellos es la forma en que se pueden interpretar sus cláusulas. Es por ello que en los <<smartcontracts>> no se admiten cláusulas ambiguas o contradictorias, tampoco podrían contener soluciones en caso de fuerza mayor o caso fortuito de los que ningún contrato está exento.<sup>27</sup>

#### **4.8.3. Jurisdicción y norma aplicable**

Aquí se nos encontramos ante una tesitura difícil de resolver, ya que como toda figura jurídica debe someterse a una ley, pero ¿ante qué ley deben responder los <<smartcontracts>>? Puesto que los contratos inteligentes han sido creados para que personas desde distintas partes del mundo puedan obligarse entre sí. Pasemos a su estudio: Como primera norma a la que se acudiría sería a lo establecido por las partes, ya que entre ellos podrían haber llegado a un acuerdo sobre ante que jurisdicción se acudiría en caso de controversia del contrato o que hubiera una cláusula arbitral añadida a este.

Pero en el supuesto de que no establecieran ante que jurisdicción deberían resolverse las controversias ni las normas aplicables, el punto de conexión podría ser la sede del contrato o donde se administra como lo proponen Bourque y Fung<sup>28</sup>, pero como ellos mismos dicen, el problema sería, que al formar parte de la <<blockchain>>, sería imposible saber dónde se ha firmado o donde es administrado, ya que no es un contrato físico ni tiene una localización específica, ya que se encontraría disperso por todos los nodos, impidiendo así determinar su jurisdicción.

Por todo esto, el legislador tanto como los creadores de contratos inteligentes, se encuentran ante un gran reto, ya que debería determinarse cuál es la legislación y la jurisdicción que ha de aplicársele a estos contratos inteligentes.

---

<sup>27</sup> Hernandez Agudelo, M. and De las Heras Ballell, T. (2017). FODERTICS 6.0 LOS NUEVOS RETOS DEL DERECHO ANTE LA ERA DIGITAL. 1st ed. GRANADA: COMARES, S.L, pp.299-303.

<sup>28</sup> Bounque, S. y Fung Ling Tsui, S. <<A lawyer's introduction to smart contracts>> Scientia Nobilitat Reviewed Studies,. 2014, págs. 4-24.

## 5. El <<bitcoin>>

Antes de comenzar a hablar específicamente sobre el <<Bitcoin>>, hablaremos en general de que son las <<criptodivisas>> o <<criptomonedas>> que son el marco donde se encuadra el <<Bitcoin>>, ya que esta es la más famosa <<criptodivisa>> pero cada día vemos como surgen nuevas (véase el ejemplo de la nueva <<criptomoneda>> sacada hace pocos días por el jugador de futbol colombiano James Rodríguez, la JR10 token<sup>29</sup>). Así que antes de entrar en el marco jurídico legal del <<bitcoin>> explicaremos brevemente en que marco está situada.

### 5.1. <<Criptodivisas o criptomonedas>>

Explicando simple y llanamente que es una <<criptomonedas>>, diremos que son monedas virtuales descentralizadas que se utilizan dentro de un sistema plenamente seguro debido a que se utiliza la criptografía en todas sus transacciones (la blockchain) y las matemáticas, aunque la terminología más adecuada para estas sería el término <<token>><sup>30</sup>. Estos <<token>> se basan en la criptografía de clave pública<sup>31</sup> que utiliza un par de claves relacionadas matemáticamente. Una transacción que es encriptada con la primera clave debe descodificarse con la segunda clave y al revés. En este sistema de claves públicas cada participante posee dos claves, por una parte, una clave es privada y debe ser secreta; por la otra, la segunda clave se podría compartir con quien se quiera, y esta sería la clave pública<sup>32</sup>.

El Banco Central Europeo a su vez, en un informe realizado en febrero de 2015 que trata sobre las monedas virtuales, las define como: “La representación digital de valor, no emitida por ninguna autoridad bancaria central, institución de crédito o emisor de dinero electrónico reconocido, que, en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero.”

### 5.2. ¿Qué es el <<bitcoin>>?

Antes de nada, me gustaría hacer una pequeña aclaración, cuando hablamos de las <<bitcoin>> en general, simplemente pensamos en ese tipo de <<criptodivisa>> del que tanto se está hablando este año, pero realmente deberíamos hacer una diferencia, ya que hablaríamos de cosas distintas si utilizamos la palabra <<Bitcoin>> (con la B en mayúscula), no es lo mismo que <<bitcoin>> (con la b en minúscula). Respecto al primer término, <<Bitcoin>>, lo utilizamos para referirnos al software y red de minería <<Bitcoin>> que se encarga de descifrar la cadena de bloques que se crean e intercambian la <<token bitcoin>>. Por su parte, <<bitcoin>> es la famosa <<criptomoneda>> que se intercambia a través del software <<Bitcoin>>.

El <<Bitcoin>> es un software que se atribuye a Satoshi Nakamoto (persona anónima de la cual aún no se sabe su identidad a día de hoy), que surgió por primera vez en el año 2008 con un mensaje titulado “Bitcoin P2P e-cash paper”<sup>33</sup>, en este explica que está

---

<sup>29</sup> Business insider. (2018). James Rodríguez saca al mercado su propia criptomoneda: el JR10 Token. [online] Available at: <https://www.businessinsider.es/james-rodriguez-saca-mercado-su-propia-criptomoneda-jr10-token-253100>

<sup>30</sup> WWW.BBVA.COM. (2017). Qué es un 'token' y para qué sirve. [online] Available at: <https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/>

<sup>31</sup> Ordovas Oromendia, J. <<Descubriendo Bitcoin: un viaje real al interior de la moneda virtual>>

<sup>32</sup> IBM Integration Bus, versión 9.0.0.2 <<Criptografía clave pública>>. [https://www.ibm.com/support/knowledgecenter/es/SSMKHH\\_9.0.0/com.ibm.etools.mft.doc/ac55940\\_.htm](https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm).

<sup>33</sup> Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [online] Nakamoto Institute. Available at: <https://nakamotoinstitute.org/bitcoin/#selection-7.4-9.38>

desarrollando un nuevo método electrónico de dinero, en el que no existe ningún tipo de intermediarios. El <<Bitcoin>> entró al mercado virtual el 11 de febrero de 2009, momento en el que se publica en la red un enlace al programa del software <<Bitcoin>>, fecha también en la que se mina el primer lote de <<bitcoins>>.

Esta tecnología del <<Bitcoin>> se ha hecho tan famosa ya que utiliza la tecnología “Peer to Peer”, la cual es una tecnología por la cual no se necesitaría de ningún intermediario para que se realizasen las transacciones.<sup>34</sup>

Lo que realmente hace seguro a este software tan innovador es la gran seguridad que transmite debido a dos elementos (los cuales ya hemos hablado en el epígrafe anterior de las criptomonedas o criptodivisas): La cadena de bloques o <<blockchain>> y el sistema de cifrado de clave pública.<sup>35</sup>

Pero continuemos centrándonos en lo que nos interesa, la <<bitcoin>> como moneda virtual. Según el informe del Banco Central Europeo sobre monedas virtuales, de 3 de mayo de 2016, afirma que aún no se ha definido este tipo de <<cibermoneda>> de manera universal, pero, la Autoridad Bancaria Europea, da a entender que podrían utilizarse a modo de representación digital de un valor, la cual no es emitida ni por ninguna administración pública ni por un banco central. Esta moneda virtual tampoco se encuentra interrelacionada con ninguna divisa fiduciaria. Pero a pesar de que aún no está regulada, esta es admitida como forma de pago entre las personas físicas y jurídicas.

Como ya hemos explicado, el <<bitcoin>> está basado en fórmulas matemáticas, las cuales no pueden ser consideradas para patentar, ni tampoco considerarse propiedad intelectual. Todo esto es lo que ocasiona que haya una falta de regulación, ya que no se sabe exactamente como encuadrar a este tipo de <<cibermoneda>>. Pero esta necesidad es urgente, como ya ha sido demostrado por el Banco Central Europeo e incluso por el mismísimo Parlamento Europeo.

### **5.3. Problemas que surgen con el <<bitcoin>>**

A continuación, describiremos una serie de problemas que están surgiendo a medida que avanza el crecimiento del <<bitcoin>> en la red, y estos problemas son los que sugieren cada vez más que haya una regulación efectiva y eficaz del <<token>> lo antes posible:

#### **5.3.1. Desestabilización del sistema financiero centralizado**

El valor de los <<bitcoins>> en comparación con el valor del dinero que circula alrededor del mundo no es equiparable, al que es emitido y reconocido por los gobiernos de todo el mundo( 1 <<bitcoin>> equivale a día de hoy a 7359.97 \$<sup>36</sup>).

Pero se han dado casos, como en Chile, lugar en el que se llegó a preferir el <<bitcoin>> para asegurar el valor de su dinero, ante una posible deflación de su moneda oficial, el Peso chileno.

Esto podría llevar a que las personas ante situaciones de posibles crisis, inviertan su dinero en <<bitcoin>> para así asegurar el valor de su dinero, provocando una grave devaluación de la moneda oficial de su país.

---

<sup>34</sup> Bitcoin, <http://bitcoin.org/es/>

<sup>35</sup> Bitcoin Wiki, FAQ, “What is mining?”, <https://en.bitcoin.it/wiki/FAQ#Mining>

<sup>36</sup> CriptoTendencia. (2018). Cotización Bitcoin online. [online] Available at: <https://criptotendencia.com/cotizacion-bitcoin-online/>

### 5.3.2. Competencia frente al sistema bancario tradicional

Otro de los motivos por los que se necesita una regulación de esta <<criptomoneda>> es debido a que esta y los sistemas bancarios prestan un servicio semejante, pero con la diferencia de que el sistema bancario este sujeto a las reglas establecidas en su país de origen además de estar supervisados por organismos gubernamentales para que su funcionamiento sea el correcto. Este no es el caso del <<bitcoin>>, que no está sometida a ningún organismo gubernamental, sino que actúa como un valor.

El problema surgiría si los ciudadanos que confían en el <<bitcoin>>, perdiesen su dinero debido a un grave desplome del <<token>> o les fuesen sustraídos, suceso que produciría que estas personas pedirían al gobierno que se aplicasen una serie de leyes para poder recuperar el dinero perdido.

### 5.3.3. Transacciones ilícitas

- Blanqueo de dinero

Como ya hemos dicho, el <<bitcoin>> funciona con la tecnología <<Blockchain>>, la protección de datos de las personas que utilizan esta tecnología es muy segura. Por este motivo debido a los problemas de lavado de dinero que ya se han encontrado en Estados Unidos<sup>37</sup>, su Departamento de lucha contra los delitos financieros, en marzo de 2013, determinó que las empresas dedicadas al intercambio de dinero debían inscribirse a este organismo y obtener licencia obligatoria para llevar a cabo sus actividades<sup>38</sup>.

- Fraude

Debido al auge del <<bitcoin>>, este interés se ha utilizado para cometer delitos de fraude engañando a personas para que invirtieran en la <<criptodivisa>> a cambio de un rendimiento futuro.

- Evasión fiscal

Otro problema que sustenta, es que debido a que como este no se encuentra todavía regulado en el sistema financiero de la mayoría de los países, se ha quedado fuera de las declaraciones fiscales (en el caso de España, Declaración del IRPF, o comúnmente llamado, Declaración de la renta)

- Narcotráfico y otras actividades ilícitas.

A lo largo del período que lleva con vida el <<bitcoin>> hemos podido ver como el tráfico de drogas ha sido habitual con esta <<criptodivisa>> debido a la privacidad que suscita. Este ha sido normalmente empleado en la “Deep web”, lugar en el que se permitía a los usuarios el intercambio de bienes ilícitos utilizando a esta <<criptomoneda>> como forma de pago.

## 5.4. Naturaleza jurídica del <<bitcoin>>

El <<bitcoin>> es una tecnología que está envuelta por una gran complejidad, pero además si a esto le unimos que se utilice como medio de pago, sin estar supeditado a ningún tipo de organismo, todo esto crea que se considere atípico y que haya una ausencia de regulación de esta tecnología. A día de hoy aún no se ha clarificado cuales son su naturaleza jurídica, siendo tres las opciones más factibles a las que relacionarlo: el título

---

<sup>37</sup> Facua, Banca, “EEUU interviene dos cuentas a la mayor operadora de moneda virtual Bitcoin, la japonesa Mt. Gox”, <https://www.facua.org/es/noticia.php?Id=7617>, última fecha de consulta el 9 de noviembre de 2014.

<sup>38</sup> Gomez Rodriguez, C. (n.d.). Derecho y Tic. Vertientes actuales. pp.272 a 275.

valor emitido en soporte electrónico, su consideración como bien mueble incorporal o software, o que se configure como una divisa electrónica de flujo bidireccional.

A continuación, vamos a analizar cuál sería la naturaleza jurídica más apropiada en la que podríamos situar al <<bitcoin>>.

#### **5.4.1. Títulos valores emitidos en soporte electrónico**

En nuestro ordenamiento jurídico no existe una definición legal de “título valor”, pero normalmente, este término se asemeja a otros como: efectos de comercio, valores negociables o valores mobiliarios. Según lo que dice Garrigues podríamos decir que el “título valor” es: “documento sobre un derecho privado cuyo ejercicio u cuya transmisión están condicionados a la posesión de documento”. Es decir, para que este tenga valor es necesaria obligatoriamente a la existencia de un documento, y que este documento esté ligado a un derecho.

Las características esenciales del “título valor” son:

- Su condición de documentos mercantiles a efectos de derecho privado
- Son títulos con legitimación propia debido a que no sería posible la ejecución del derecho establecido sin la presentación por el acreedor. Como el <<bitcoin>> no está regulado en nuestro ordenamiento, no existe un reconocimiento legal de que incorpore un derecho
- Son títulos que atribuyen al derecho en ellos descrito o incorporado un carácter literal y autónomo, depende del título únicamente<sup>39</sup>.

Los “títulos valores” son considerados bienes muebles, por ello, tienen carácter de ser poseídos en sentido estricto y de transmisión mediante los métodos establecidos en nuestro ordenamiento.

Dentro de la categoría de “títulos valores” habría que establecer a que rama pertenece el <<bitcoin>>: a los emitidos individualmente o a los emitidos en masa.

Los “títulos valores” emitidos individualmente se producen al amparo de una única operación, elemento que no se ajusta al tipo de operación que se realiza con el <<bitcoin>>. Por otra parte, los “títulos valores” emitidos individualmente con soporte electrónico no presentan una relación de fungibilidad con otros títulos de la misma clase. Para defender la idea de equiparar al <<bitcoin>> como “título de valor” emitido en soporte electrónico, podrían ser utilizados los apartados cuatro y siete del artículo tres de la Ley 59/2003, de 19 de diciembre, de firma electrónica que dicen:

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable<sup>40</sup>.

Entendemos de estos dos apartados que la firma electrónica no modifica los requisitos legales exigidos independientemente del documento electrónico del que se trate. Esto quiere decir, que debido a que el <<bitcoin>> no tiene cabida en nuestra legislación, la legalidad de la firma electrónica no dará la condición de “título de valor” emitido en soporte electrónico.

---

<sup>39</sup> Chulia, F.V.: Introducción al derecho Mercantil, Tirant lo Blanch, Valencia, 21ª edición, 2008, págs. 1.184 y ss

<sup>40</sup>Jefatura del Estado. (2003). Ley 59/2003, de 19 de diciembre, de firma electrónica.

De esta manera, concluimos que el <<bitcoin>> no es posible encuadrarlo en el campo de “título de valor” con soporte electrónico emitido individualmente.

Por otro lado, los “títulos valores” emitidos en masa, también denominados instrumentos financiero, Zunzunegui los sugiere como: “todo valor negociable o contrato susceptible de negociación organizada en el mercado de valores”<sup>41</sup>.

Todo esto interconecta la idea de “instrumento financiero” con el de “título valor negociable”, cuyo concepto viene regulado en el art.2.1 del Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del mercado de valores que dice:

1. Los valores negociables emitidos por personas o entidades, públicas o privadas, y agrupados en emisiones. Tendrá la consideración de valor negociable cualquier derecho de contenido patrimonial, cualquiera que sea su denominación, que por su configuración jurídica propia y régimen de transmisión, sea susceptible de tráfico generalizado e impersonal en un mercado financiero<sup>42</sup>.

Este apartado del artículo 2, incluye tanto instrumentos monetarios, valores negociables típicos y valores atípicos.

Pero a pesar esto, el <<bitcoin>> es una metodología de pago, y los medios de pago no están incluidos como valores negociables, como ya hemos podido comprobar.

Por todas estas motivaciones podríamos considerar que el <<bitcoin>> no pertenecería a ninguna de las categorías aquí descritas, y por lo tanto no tendría la naturaleza jurídica de títulos valores emitidos en soporte electrónico.

#### **5.4.2. El <<bitcoin>> como bien inmueble incorpóreo**

Cuando hablamos de <<Bitcoin>> como software, es difícil su clasificación, ya que aún no se ha esclarecido en el tema, si el software está dentro de la propiedad industrial o propiedad intelectual<sup>43</sup>.

Lo que hay que tener claro, es que, aunque este programa informático, este almacenado en un soporte físico, se trata de un bien intangible. Podríamos incluirlo en la categoría de bienes muebles inmateriales, así podemos deducirlo del apartado 335 de nuestro Código Civil el cual dice:

“Se reputan bienes muebles los susceptibles de apropiación no comprendidos en el capítulo anterior, y en general todos los que se pueden transportar de un punto a otro sin menoscabo de la cosa inmueble a que estuvieren unidos.”<sup>44</sup>

Estos softwares están regulados y protegidos en el Real Decreto legislativo 1/1996, de 12 de abril, en su artículo 10.1 i):

“1. Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:

- i) Los programas de ordenador.”<sup>45</sup>

---

<sup>41</sup> Zunzunegui Pastor, F., op. Cit., págs. 169 y ss.

<sup>42</sup> Jefatura del Estado. (2015). Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores.

<sup>43</sup> Davara Rodríguez, M. A.: Manual de Derecho Informático, Aranzadi, 11.ª edición, 2015, pág.120.

<sup>44</sup> Ministerio de Gracia y Justicia. (1889). Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

<sup>45</sup> Ministerio de Cultura. (1996). Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

La Unión Europea en la Directiva 91/250/EEC, sobre la protección legal de programas informáticos de 1991, en su artículo 1.1, establece que los programas informáticos son obras literarias, así como el material que se utiliza para su diseño<sup>46</sup>.

Cuando nos referimos al supuesto de la adquisición de <<bitcoin>> hablamos de una compra porque lo que estamos obteniendo es una copia del software. Esta situación es la más común cuando se realizan transacciones para adquirir programas a través de internet<sup>47</sup>; un claro ejemplo de esto podríamos verlo en plataformas de videojuegos como Steam, en la que se paga una cantidad de dinero determinada, para adquirir una copia del videojuego y se hace una copia en el disco duro, sin necesidad de tener el formato físico de dicho programa.

En base a esta posición, podríamos decir que el tipo de contrato que se realiza al utilizar <<bitcoins>>, el más similar sería el de la permuta, el cual viene recogido en el artículo 1538 del Código civil:

“La permuta es un contrato por el cual cada uno de los contratantes se obliga a dar una cosa para recibir otra.”<sup>48</sup>

Esto quiere decir, que en la transacción lo que sucedería es que una persona da X <<bitcoins>> establecidos previamente, mientras la otra se obliga a dar otra cosa determinada.

Pero a pesar de todo ello, a día de hoy, los <<bitcoins>> su objetivo y finalidad es la de ser un medio de pago, por esto, parece que esta <<criptodivisa>> no podríamos encuadrarlo como un bien inmueble y por lo tanto no pertenecería a este marco jurídico.

#### **5.4.3. El <<bitcoin>>: Divisa virtual de flujo bidireccional**

En nuestra legislación, no encontramos ninguna definición clara de que es una <<divisa>>, tanto el Código Civil, tanto como el Código de Comercio, hablan sobre esta materia, pero en ningún momento lo definen de una manera eficaz.

Una definición de divisas, sería la expuesta por el Fondo Monetario Internacional, el cual dice: «Las divisas incluyen los títulos de crédito de las autoridades monetarias frente a no residentes en forma de depósitos bancarios, letras de tesorería, valores públicos a corto y largo plazo, unidades monetarias europeas y otros títulos de crédito utilizables en caso de déficit de balanza de pagos, incluidos los títulos de crédito no negociables provenientes de acuerdos entre bancos centrales o entre gobiernos, con independencia de que estén denominados en la moneda del país deudor o acreedor»<sup>49</sup>.

Debido a la creación del Euro en 1999 y posteriormente puesta en circulación en 2002 como medio de pago único en la zona Euro, propició la creación de una regulación de una regulación uniforme de los instrumentos de pago que posibilitarían el aprovechamiento de la moneda europea por excelencia.

El Banco Central Europeo hace una diferenciación entre tres clases de divisa virtual:

---

<sup>46</sup> Rosembuj, T.: «El programa informático». Revista Quincena Fiscal, n.º 21, 2008, parte Estudio Editorial Aranzadi, SA, Cizur Menor, pág. 8.

<sup>47</sup> García Novoa, C.: «Consideraciones sobre la Tributación del Comercio Electrónico (II)», Revista Quincena Fiscal, n.º 16/2001, parte Doctrina, Editorial Aranzadi, SA, Pamplona, pág. 21.

<sup>48</sup> Ministerio de Gracia y Justicia. (1889). Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

<sup>49</sup> El Fondo Monetario Internacional, como observamos, defiende la naturaleza de la divisa con independencia a su reconocimiento como moneda en el país deudor o acreedor. Acceso en fecha 14 de junio de 2016, en la dirección: <http://www.imf.org/external/spanish/pubs/ft/bop/2007/bopman6s.pdf>

- Divisas in-game only: Este tipo de divisas son aquellas que se crean y se utilizan explícitamente para aquellos entornos para los que son creadas, y no podrían utilizarse fuera de ese ámbito. Un claro ejemplo son los videojuegos de los teléfonos móviles, en los cuales, si quieres obtener más facilidades o customizar a tus personajes, necesitarías de este tipo de <<token>>.
- Divisas virtuales unidireccionales: Son aquellas divisas que se obtienen de manera virtual, mediante el pago de divisa tradicional y una vez realizada la transacción, esta no se puede revertir.
- Divisas virtuales bidireccionales: Este supuesto, a diferencia del anterior si permitiría una transformación desde la divisa virtual a la divisa tradicional.

Hemos de aclarar aquí, que las divisas virtuales bidireccionales no es considerado dinero electrónico, puesto que el dinero electrónico tiene reconocimiento legal tanto en el tratado de Lisboa, en su artículo 128, así como su regulación en la Ley 21/2011, de 26 de julio, de dinero electrónico. El termino >>dinero electrónico>>, fue definido por el Banco Central Europeo, en el informe que realizó en 1998, que lo define de la siguiente manera: «valor monetario almacenado electrónicamente en un dispositivo tecnológico que puede ser usado para realizar pagos a cualquier empresa distinta del emisor sin necesidad de involucrar cuentas bancarias en la transacción, pero actúa como instrumento pre- pagado al portador»<sup>50</sup>.

En la Ley 21/2011, de 26 de julio, de dinero electrónico, este es considerado en su artículo 1.2:

“Se entiende por dinero electrónico todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico.”<sup>51</sup>

En base a esta definición, es claro que el <<bitcoin>> no entra dentro de ella, todo ello debido a que, en contraposición del dinero electrónico, el <<bitcoin>> no se expresa en ninguna unidad monetaria legal, sino en una unidad virtual que es el <<bitcoin>>.

Por lo que, debido a todo lo expuesto anteriormente, tampoco podríamos establecer al <<bitcoin>> dentro de esta naturaleza jurídica, ya que no encuadra en ninguna de las formas de divisas virtuales mencionadas anteriormente.

## 5.5. Marco legislativo

En la actualidad, seguimos sin que exista ninguna legislación específica a esta materia. Por su parte, la Unión Europea ha mostrado mucho interés para tomar medidas y así evitar determinados delitos relacionados con esta <<criptodivisa>> (blanqueo de capitales, compra de drogas...). Todo esto viene como consecuencia del informe emitido por el Banco central Europeo, el 25 de Febrero de 2025, referido a las monedas virtuales. A través de este informe se advierte a las autoridades nacionales europeas, que estas no se encuentran reguladas, por lo que deberían adaptar la legislación ya existente para que fueran aplicables a estas <<civerdivisas>><sup>52</sup>.

<sup>50</sup> Acceso en fecha 14 de junio de 2016, en la dirección: <https://www.ecb.europa.eu/pub/pdf/annrep/ar1998es.pdf?36bedac73b198b96cd7f03d2b26e0ba>

<sup>51</sup> Ley 21/2011, de 26 de julio, de dinero electrónico. (2011). «BOE» núm. 179, de 27 de julio de 2011, páginas 84235 a 84254 (20 págs.).

<sup>52</sup> Esquemas de moneda virtual - un análisis adicional. (2015). [Ebook]. Alemania. Retrieved from <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

## **5.6. El <<bitcoin>> en el proceso penal**

Debido a que este <<token>> (no es el único) utiliza la tecnología <<blockchain>> es muy difícil saber quién es el titular de estas divisas virtuales, además esto se complica aún más, ya que, se pueden transferir fácilmente desde dos puntos muy alejados (como puede ser de España a Estados Unidos). Esto ha facilitado, que en páginas webs que se dedican a la ejecución de actividades ilícitas.

Con motivo de estas ilicitudes, la policía se encuentra ante la ardua tarea de localizar a quien es el titular que se encuentra detrás de tales transacciones.

### **5.6.1. ¿Cómo relacionar el <<bitcoin>> a su titular?**

Podríamos decir, que existen cuatro maneras de identificar al titular del <<bitcoin>> con su transacción ilegal.

- A través de su publicación en internet: Estas pueden publicarse, por ejemplo, cuando se hace algún tipo de donativo a través de esta divisa virtual. Esta dirección quedaría guardada, que posteriormente podría ser buscada mediante un motor de búsqueda especializado.
- Conversión de <<bitcoin>> a moneda legal: Esta acción tiene que realizarse a través de una casa de cambio o exchange que se dedique a la compraventa de <<bitcoin>>. Estos negocios, están sometidos a diversas leyes tanto nacionales, como internacionales, por eso para prevenir el blanqueo de dinero, exigen que las personas que vayan a utilizar sus servicios se identifiquen de manera veraz. Así, los denominados exchanges, conocerían la identidad de la dirección pública del <<bitcoin>>.
- Monedero virtual. Estos, son servidores web que ofrecen un servicio de almacenaje, por lo que deben conocer las direcciones de <<bitcoin>> además de aquella información que crean necesaria para su identificación.
- Proveedores de servicios de internet: Debido a que estos son los encargados de proporcionar internet a los clientes, ellos controlan el tráfico, así que pueden analizar ese tráfico y saber cuál es la dirección del <<bitcoin>> (pero este no es del todo fiable debido a que usuarios con más conocimiento en la materia “hacking” podrían encubrir esta dirección a través de diversos medios como Tor o VPN)<sup>53</sup>

### **5.6.2. El registro remoto en los equipos informáticos**

Esta forma de motorización de un ordenador, es indudablemente una gran noticia para las fuerzas del orden, debido a que debido a la nueva legislación, el juez podría autorizar a la policía judicial, a introducir un troyano en el ordenador que se quiere investigar sin el previo consentimiento de su dueño<sup>54</sup>, pero esta actuación solo podría llevarse a cabo cuando sea alguno de los delitos enumerados en el artículo 588 septies a presupuestos, apartado e:

---

<sup>53</sup> Kryskova Kuksa, T. (2017). Fodertics 6.0 Los nuevos retos del derecho ante la era digital (1st ed., pp. 313 a 322). Granada.

<sup>54</sup> Conde-Pumpido Tourón. C., La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos

"Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación."<sup>55</sup>

Por lo tanto, según lo establecido en el artículo anteriormente citado, cabría la posibilidad de utilizar este método, cuando se realicen delitos en los que se haya utilizado el <<bitcoin>>.

Así a través de esta medida, podría utilizarse para averiguar la dirección del <<bitcoin>> y asociarlas a su titular aparte de poder encontrar las contraseñas que se utilizan para acceder a los monederos de los que es dueño el usuario y examinar las transacciones realizadas.

Esta acción remota, tiene una duración máxima de un mes, pero prorrogable dos veces más por una duración idéntica hasta llegar al máximo de tres meses.

### **5.6.3. Registro de almacenamiento masivo de información**

Esta acción corresponde con el acceso a la información contenida en todo tipo de dispositivos multimedia, puesto que en estos es posible encontrar información relacionada a la dirección <<bitcoin>> o de los monederos, así como las claves de acceso. Como en el caso anterior sería necesaria la previa autorización judicial para poder incautar este tipo de dispositivo y posteriormente analizarlo en búsqueda de las citadas direcciones o claves. Pero existe la posibilidad de incautar dichos bienes sin la necesidad de esa autorización, en aquellos casos de extrema urgencia, que vienen establecidos en el artículo 588 sexies c. Autorización judicial párrafo 4 de la Ley Criminal:

“En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.”<sup>56</sup>

---

<sup>55</sup> Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (1882). «BOE» núm. 260, de 17/09/1882.

<sup>56</sup> Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (1882). «BOE» núm. 260, de 17/09/1882.

## 6. Eficacia probatoria de la <<Blockchain>>

Es común ver la afirmación de que el registro documental en la <<blockchain>> es jurídicamente válido o que tiene validez legal, pero si nos redirigimos a la definición expuesta por la Real Academia Española, válido significa:

“Firme, subsistente y que vale o debe valer legalmente.”<sup>57</sup>

Pero habríamos de hacer una aclaración, ya que, más que validez legal, esta cadena de bloques serviría como una prueba legal de las transacciones registradas en ella, puesto que esta no tendría validez ya que no está regulada ni estipulada en ninguno de nuestros ordenamientos.

Este tipo de “prueba” sería válido debido a lo que establece el artículo 299 de la Ley de Enjuiciamiento Civil, en su apartado tercero expone:

“Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.”<sup>58</sup>

Al considerarse este un medio de prueba eficaz, vendría constitucionalmente protegido en el artículo 24.2 de la Constitución Española, el cual establece:

“[...]a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.”<sup>59</sup>

Por lo tanto, podríamos decir, que la <<blockchain>> es válidamente considerado un medio de prueba legal.

### 6.1. Valor jurídico del sellado de tiempo. Clases de sellos de tiempo.

Cuando se realiza una transacción que se introduce en la <<blockchain>>, cuando se introduce, se produce un sellado de tiempo. Cada vez que se produce una acción y se registra, esta produce un <<hash>> (el cual ya hemos explicado en el apartado introductorio)<sup>60</sup>.

En Norteamérica, ya incluso podemos encontrar jurisprudencia que trata sobre este tema, y admiten el valor de prueba legal de la función <<hash>><sup>61</sup>. A pesar de ellos no existe jurisprudencia, que acepte el valor probatorio del registro de la <<blockchain>>, ya que realiza la misma función que el <<hash>>, con la única diferenciación de que no existe ningún tercero que lo verifique, sino que es el propio sistema.

En nuestro ordenamiento, podríamos ver una pequeña aproximación, en el Reglamento Europeo de Firma Electrónica 910/2014 de 23 de julio, en su artículo 41 que dice:

“A fin de garantizar la sostenibilidad y durabilidad de los servicios de confianza cualificados y de potenciar la confianza de los usuarios en la continuidad de dichos servicios, los organismos de supervisión deben verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese en caso de que los prestadores cualificados de servicios de confianza cesen en sus actividades.”<sup>62</sup>

<sup>57</sup> Diccionario de la lengua española. Retrieved from <http://dle.rae.es/?id=bIy6PkC>

<sup>58</sup> Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (2000). «BOE» núm. 7, de 08/01/2000.

<sup>59</sup> Constitución Española. (1978). «BOE» núm. 311, de 29/12/1978.

<sup>60</sup> ¿QUÉ ES UNA CADENA DE BLOQUES (BLOCK CHAIN)?. Retrieved from <https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/>

<sup>61</sup> Lorraine et al. v. Markel American Insurance Company (IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND 2007).

<sup>62</sup> REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones

En otras palabras, se necesitaría de un Prestador de Servicios de Confianza que diese validez a esta prueba legal, pero en el caso de la <<blockchain>> carece de este ente, por lo que habrá que acreditar esa validez, ante el Juez o Tribunal, de manera que se demuestre que el <<hash>> producido por la acción que ha tenido lugar en la <<blockchain>> no ha sido alterado desde una fecha concreta.

## **6.2. Actividad probatoria**

Debido a que la <<blockchain>> utiliza un lenguaje informático que no es comprensible si no se es especialista en dicha materia, sería necesaria una prueba pericial para determinar que esta prueba es válida, esta prueba se hará conforme a lo establecido en la Ley de Enjuiciamiento Civil en sus artículos 335 y siguientes.<sup>63</sup>

Una vez que es el Juez acepta esta validación, habremos de hablar de los aspectos jurídicos, ya que la eficacia que tenga este tipo de prueba dependerá del contenido y de la titularidad del archivo.

En relación a los documentos electrónicos, la Ley de Enjuiciamiento Civil, en su artículo 326, establece que se deberá actuar según lo dispuesto en el artículo 3 de la ley de Firma electrónica<sup>64</sup>, pero esta ha sido derogada por el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, en el que explica en su artículo 49:

“El presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada. Sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita.”

En el caso de que no exista firma electrónica reconocida, podría servir como recambio o sustitución de esta, cualquier otra modalidad de firma, marca o sello digital, como bien establece el artículo 326 de la Ley de Enjuiciamiento Civil.

## **6.3. Utilizando la <<blockchain>> como registro de la propiedad intelectual**

Es común que surjan noticias sobre la utilización de esta innovadora tecnología como Registro de propiedad intelectual o industrial, ya que el bloque que se crea y se anexa, puede contener cualquier tipo de cosa, desde un software de ordenador, hasta una obra literaria, etc.

Pero a pesar de que esta estuviera hecha en la cadena de bloques, no garantizaría la titularidad de lo que se quiere registrar, no serviría como prueba, es decir, que no se podría apelar a la presunción establecida en el artículo 145 de la Ley de Propiedad Intelectual en su apartado número 3:

“Se presumirá, salvo prueba en contrario, que los derechos inscritos existen y pertenecen a su titular en la forma determinada en el asiento respectivo.”<sup>65</sup>

---

electrónicas en el mercado interior (2014). «DOUE» núm. 257, de 28 de agosto de 2014, páginas 73 a 114 (42 págs.).

<sup>63</sup> Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (2000). «BOE» núm. 7, de 08/01/2000.

<sup>64</sup> Ley 59/2003, de 19 de diciembre, de firma electrónica. (2003). «BOE» núm. 304, de 20/12/2003.

<sup>65</sup> Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. (1996). «BOE» núm. 97, de 22/04/1996.

La única forma por la que se podría entender como legal algún registro de propiedad intelectual en la <<blockchain>> sería mediante la inclusión de una firma digital del autor en ese bloque, que sería inmutable. De esta forma, si se incluye la firma del autor en el bloque donde se registra esa propiedad intelectual, el Juez o Tribunal, tendría que atenerse a lo establecido en el artículo 6.1 de la Ley de propiedad intelectual que dice:

“Se presumirá autor, salvo prueba en contrario, a quien aparezca como tal en la obra, mediante su nombre, firma o signo que lo identifique”

De hecho, ya existen <<startups>>, que se dedican exclusivamente al registro de la propiedad intelectual o industrial en la <<blockchain>>. Este es el caso de Leftherian<sup>66</sup>, que nació con la idea de almacenar en la <<blockchain>> la información de identificación de obras artísticas, junto con la firma digital del autor, de modo que los autores puedan tener un respaldo seguro, en el que se demuestre el momento exacto de la inscripción de su creación.

#### **6.4. <<Blockchain>> en el ámbito sucesorio**

También es usual ver cada día nuevas referencias ante la posibilidad del uso de la cadena de bloques como medio de certificación de testamentos sin la intervención de los notarios. El único caso en el que sería útil la utilización de la <<blockchain>> para validar una sucesión, sería en el caso de los testamentos ológrafos, puesto que estos no necesitan de notario para ser redactados. Pero incluso en estos casos, no sería suficiente el registro en la cadena de bloques, puesto que según como establece el artículo 688 del Código Civil: “Para que sea válido este testamento deberá estar escrito todo él y firmado por el testador, con expresión del año, mes y día en que se otorgue.”<sup>67</sup>

A pesar de lo que se pueda pensar, la jurisprudencia exige el carácter manuscrito del testamento, por lo que, aunque la firma electrónica si se consideraría válida, faltaría un elemento esencial, que es el propio documento escrito en sí.

Por otra parte, aunque se escribiera este documento de una manera escrita, se firmase, se escaneará y se adjuntase a la <<blockchain>> sería también esencial la tenencia del manuscrito que ha sido escaneado para que este obtuviera valor legal<sup>68</sup>.

Por lo tanto, a día de hoy la tecnología de la cadena de bloques no podría utilizarse en este ámbito, pero no es de extrañar que un futuro no muy lejano, las legislaciones se adapten a dichas tecnologías, quizás no como una figura principal, pero quizás como una complementaria que facilite el trabajo a los notarios y a las personas que quieran realizar este tipo de testamentos electrónicos.

---

<sup>66</sup> García, C. (2017). LEFATHERIAN: EL FUTURO DE LA PROPIEDAD INTELECTUAL BASADO EN BLOCKCHAIN. Retrieved from <https://www.criptonoticias.com/entrevistas/leftherian-futuro-propiedad-intelectual-basado-blockchain/>

<sup>67</sup> Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. (1889). «BOE» núm. 206, de 25/07/1889.

<sup>68</sup>Gonzalez Granado, J. (2016). Eficacia probatoria de la blockchain. Retrieved from <https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/>

## 7. Reflexiones finales

Como hemos podido ver la tecnología <<blockchain>> cada vez abarca más temas relacionados con el derecho y por ello es indispensable darle una cavidad desde el punto de vista jurídico para que se pueda utilizar de una forma legal.

En este trabajo, hemos aplicado esta tecnología en base al ordenamiento jurídico actual, enmarcándolo de la forma más correcta posible (esto no quiere decir, que no se necesite de un estudio más específico sobre la materia para adaptarlo aún más y mejor, porque debido a esta falta de legislación no se puede aprovechar al 100% esta innovadora tecnología).

Por lo tanto, aquí hemos definido y explicado de una manera sencilla en que consiste la <<blockchain>> y cuales es el futuro que tiene por delante, ya que podrá ser utilizada en numerosos ámbitos dando lugar a una transparencia más eficaz y fiable, resolviendo el problema de la desconfianza que hoy día sigue relacionado con el tema de las acciones en línea.

Respecto al derecho al olvido, hemos propuesto varias soluciones que hoy día se estudian, debido a la imposibilidad de mutar o cambiar el bloque ya introducido en la cadena, como la cadena de bloques editable (que cada vez cobra más fuerza), y permitiría así ejercer este derecho al olvido, que no es más ni menos que un derecho constitucional, por lo que, si no se pudiera modificar ese bloque, estaríamos atentando contra la intimidad de una persona.

Otro tema tratado, es el relacionado a los <<smartcontracts>>. En este tema, la <<blockchain>> puede hacer que olvidemos los contratos tradicionales como los conocemos, debido a que supondría una gran revolución y aportaría una gran seguridad jurídica a los contratantes. Todo ello debido a que, gracias a ellos, podrían crearse infinidad de nuevas modalidades contractuales, en las que solo se necesitaría, la firma digital de ambos contratantes y que establezcan las condiciones del contrato, y una vez que se cumplan estas condiciones, el contrato se ejecutaría de manera automática, sin la necesidad de ningún intermediario, y aportando la seguridad, de que ninguna de las partes puede ser estafada ya que hasta que no se cumplan las condiciones expuestas, este no se ejecutaría.

De todo esto no podríamos hablar, si no fuese por la <<criptodivisa>> <<bitcoin>>. Esta divisa virtual, tare de cabeza a los Bancos Centrales, porque cada vez más y más gente, utiliza o es poseedor de esta moneda. Además, cada día salen en las noticias nuevos casos, en los que es posible adquirir bienes a cambio de esta <<cibermoneda>>, por eso como bien hemos expuesto, podríamos considerar a esta como una divisa virtual bidireccional, que, aunque no es considerada como dinero electrónico por los Bancos Centrales (aún), estos organismo no deberían de dejar de lado a esta divisa bidireccional, porque cada vez más ciudadanos la consideran como una forma de pago, y está a evocada a sustituir y reemplazar a la moneda tradicional tal y como la conocemos, ya que el dinero físico está condenado a desaparecer (véase el incremento de utilización de tarjetas de crédito).

Por último, hemos estudiado sobre el carácter probatorio de la <<blockchain>> que como hemos podido comprobar, que es una tecnología en auge, sobre todo en el ámbito del registro, debido a su característica principal que es la inmutabilidad siempre y cuando pueda reconocerse la autoría a través de un elemento identificativo como es la firma electrónica.

Por todo esto, creo que la <<blockchain>> es algo que tiene que tener y ya tiene cabida en nuestro derecho, es una realidad, de la que tienen que comenzar a aplicar los distintos ordenamientos, ya que es una herramienta que pueda facilitar la credibilidad y la seguridad jurídica en muchos ámbitos.

## 8. Bibliografía

- ¿Qué es Blockchain o Cadena de Bloques?: <https://www.economiasimple.net/que-es-blockchain-o-cadena-de-bloques.html>
- ¿Qué es la Cadena de Bloques (Blockchain)?. [Blog]: <https://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/>
- Pastor, J. (2017). Qué es blockchain: la explicación definitiva para la tecnología más de moda: <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>
- Sentencia contra el caso Google. (2014): <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&ampageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=276332>
- Perez, I. (2017). BLOCKCHAIN Y DERECHO AL OLVIDO: ELIMINANDO DATOS DE LA CADENA: <https://www.criptonoticias.com/regulacion/blockchain-derecho-olvido-eliminando-datos-cadena/>
- Garcia Zarzalejos, A. (2017). Bruselas, tenemos un problema: el 'blockchain' choca con la normativa de datos: [https://www.elconfidencial.com/economia/2017-04-30/tecnologia-disruptiva-blockchain-cadena-bloques-derecho-al-olvido-reglamento-proteccion-datos\\_1363610/](https://www.elconfidencial.com/economia/2017-04-30/tecnologia-disruptiva-blockchain-cadena-bloques-derecho-al-olvido-reglamento-proteccion-datos_1363610/)
- Ros, E.(2018). Blockchain vs Derecho al olvido: <https://www.bonattipenal.com/blockchain-vs-derecho-al-olvido/>
- Frías García, V. (24 de junio, 2016). Smart contracts, ¿el futuro del blockchain? [artículo de blog]. :<http://www.intelygenz.es/smart-contracts-el-futuro-del-blockchain/>
- mi ethereum. (2018). SMART CONTRACTS O CONTRATOS INTELIGENTES: <https://miethereum.com/smart-contracts/>
- ¿Qué son los contratos inteligentes o smart contracts? Bitcoin y Ethereum o el dinero programable. (2015).: <https://www.oroynfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/>
- <http://bithalo.org/>
- <https://www.blackhalo.com/>
- Prenafeta Rodriguez, J., (15 septiembre, 2016). Smart contracts: aproximación al concepto y problemática legal básica [artículo de blog]:<http://diarilolaley.laley.es>.
- Hernandez A., (03 octubre, 2016). Pronto firmarás contratos irrompibles que aseguran su propio cumplimiento. [artículo de blog].: [http://www.eldiario.es/hojaderouter/internet/contratos\\_inteligentes-smart\\_contracts-tecnología-blockchain-derecho\\_0\\_564494160.html](http://www.eldiario.es/hojaderouter/internet/contratos_inteligentes-smart_contracts-tecnología-blockchain-derecho_0_564494160.html)
- Bussines insider. (2018). James Rodríguez saca al mercado su propia criptomoneda: el JR10 Token. [online]: <https://www.businessinsider.es/james-rodriguez-saca-mercado-su-propia-criptomoneda-jr10-token-253100>
- WWW.BBVA.COM. (2017). Qué es un 'token' y para qué sirve. [online]: <https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/>
- IBM Integration Bus, versión 9.0.0.2 <<Criptografía clave pública>>. [https://www.ibm.com/support/knowledgecenter/es/SSMKHH\\_9.0.0/com.ibm.etools.mft.doc/ac55940\\_.htm](https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm).
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [online] Nakamoto Institute. <https://nakamotoinstitute.org/bitcoin/#selection-7.4-9.38>
- Bitcoin, <http://bitcoin.org/es/>

- CriptoTendencia.(2018). Cotización Bitcoin.: <https://criptotendencia.com/cotizacion-bitcoin-online/>
- Facua, Banca, “EEUU interviene dos cuentas a la mayor operadora de moneda virtual Bitcoin, la japonesa Mt. Gox”, <https://www.facua.org/es/noticia.php?Id=7617>,
- El Fondo Monetario Internacional, como observamos, defiende la naturaleza de la divisa con independencia a su reconocimiento como moneda en el país deudor o acreedor: <http://www.imf.org/external/spanish/pubs/ft/bop/2007/bopman6s.pdf>
- Esquemas de moneda virtual - un análisis adicional. (2015). [Ebook]. <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- Gonzalez Granado, J. (2016). Eficacia probatoria de la blockchain. Retrieved from <https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/>
- Boletín oficial del Estado. (1978). Constitución española.
- Peces Barba, G.: Derechos Fundamentales.
- Davara Rodriguez, M. (2015). Manual de Derecho informático
- Davara, M.A.: <<Intimidad, informática y seguridad jurídica en España>>, Boletín de la Fundación para el Desarrollo Social de las Comunicaciones (128) FUDNESCO.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (1999).
- Alvarez Caro, María, Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital,
- Mendoza Enriquez, O. (2017). Fodertics 6.0: Los nuevos retos del derecho ante la era digital
- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. (1889).
- Szabo, N (1 septiembre 1997). <<Formalizing and securing relationships on public networks>>. Peer-reviewed journal on the internet.
- Christindis, K y Devetsikiotis, M. (10 de mayo, 2016). <<Blockchains and Smart contracts for the internet of things>>.
- Bounque, S. y Fung Ling Tsui, S. <<A lawyer’s introduction to smart contracts>> Scientia Nobilitat Reviewed Studies,.
- Ordovas Oromendia, J. <<Descubriendo Bitcoin: un viaje real al interior de la moneda virtual>>
- Gomez Rodriguez, C. (n.d.). Derecho y Tic. Vertientes actuales.
- Chulia, F.V.: Introducción al derecho Mercantil, Tirant lo Blanch
- Jefatura del Estado. (2003). Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Jefatura del Estado. (2015). Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores.
- Ministerio de Cultura. (1996). Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Rosembuj, T.: «El programa informático». Revista Quincena Fiscal, n.º 21, 2008
- García Novoa, C.: «Consideraciones sobre la Tributación del Comercio Electrónico (II)», Revista Quincena Fiscal, n.º 16/2001
- Ley 21/2011, de 26 de julio, de dinero electrónico. (2011). «BOE» núm. 179, de 27 de julio de 2011,

- Conde-Pumpido Tourón. C., La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (1882). «BOE» núm. 260, de 17/09/1882.
- Diccionario de la lengua española.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (2000). «BOE» núm. 7, de 08/01/2000.
- Lorraine et al. v. Markel American Insurance Company (IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND 2007).
- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (2014). «DOUE» núm. 257, de 28 de agosto de 2014