Universidad de Oviedo

FACULTAD DE ECONOMÍA Y EMPRESA

PCEO en Derecho y Administración y Dirección de Empresas.

Curso 2019/2020

Criptomonedas y Tecnología Blockchain

Autor: Marta Sánchez González

Oviedo, Mayo de 2020

RESUMEN/ABSTRACT

Resumen: En el este trabajo hemos analizado los cambios a los que está asistiendo la sociedad hoy en día en cuanto al sistema financiero se refiere, en concreto, al mercado del dinero. Gracias a internet es posible comunicar y trasladar información al instante desde diferentes puntos de la tierra. Uno de estos grandes avances que hemos visto es la aparición de las criptomonedas apoyadas en la tecnología blockchain, lo que nos hace estar presentes en el paso del Internet de la información a internet del valor

Dada la importancia de la blockchain, nos hemos detenido en dicha tecnología para explicar su funcionamiento, su irrupción dentro del sistema financiero y sus posibles aplicaciones.

Además, dentro del campo de las criptomonedas, hemos analizado la más popular hasta la fecha, el bitcoin, con sus usos, sus principales rasgos y todo aquello que deba ser destacado.

Por último, hemos definido el Ethereum, la otra gran criptomoneda y su principal aplicación, los “Smart contracts” y las ICO.

Palabras clave: dinero, blockchain, bitcoin, criptomoneda.

Abstract: In the following work we have analysed the changes that society is witnessing today as regards the financial system, in particular the money market. Thanks to the internet it is possible to communicate and transfer information instantly from different points of the earth. One of these great advances that we have seen is the appearance of cryptocurrencies supported by blockchain technology.

We have stopped at this technology to explain its operation, and its possible applications.

In addition, within the field of cryptocurrencies we have analyzed the most popular to date, bitcoin with its uses, its main features and everything that should be highlighted.

Finally, we have defined the Ethereum, the other great cryptocurrency and its main application, the Smart contracts and the ICOs.

Índice

1. INTRODUCCIÓN 4
2. HISTORIA DEL DINERO: DEL TRUEQUE A LA APARICIÓN DEL DINERO ELECTRÓNICO 5
3. EL PAPEL DEL DINERO ELECTRÓNICO EN LA ECONOMÍA ACTUAL 6
4. LA APARICION DEL BITCOIN Y LA TECNOLOGÍA ASOCIADA 8
5. TECNOLOGÍA BLOCKCHAIN 10
5.1 BLOCKCHAIN PÚBLICA Y PRIVADA 14
5.2 ELEMENTOS BASICOS DE LA TECNOLOGIA BLOCKCHAIN Y SU SEGURIDAD 14
6. CRIPTOMONEDAS: ASPECTOS GENERALES 15
6.1 ¿CÓMO SE COMPRA O SE INVIERTE EN CRIPTOMONEDAS? 17
6.2 REGULACIÓN LEGAL 18
7. ASPECTOS PRÁCTICOS EN EL USO DEL BITCOIN 18
7.1 CARACTERISTICAS PRINCIPALES DEL BITCOIN 18
7.2 EL PRECIO DEL BITCOIN 19
7.3 LA ADQUISICION DE BITCOINS 20
7.4 ASPECTOS PRÁCTICOS EN EL USO DEL BITCOIN: EL MONEDERO DIGITAL 21
7.5 COMO ACCEDER A LA COMUNIDAD BITCOIN 23
7.5.1. Algoritmos de Hashing 23
7.6. SEGURIDAD Y RIESGOS 24
8. LOS SMART CONTRACTS LIGADOS A ETHEREUM 25
9. APLICACIONES DE LA TECNOLOGIA BLOCKCHAIN 26
9.1 BANCA 27
9.2 ASEGURADORAS 29
9.3. OTRAS POSIBLES APLICACIONES 30
10. NUEVAS FORMAS DE FINANCIACIÓN EMPRESARIAL: LAS ICO 30
11. CONCLUSIONES 32
BIBLIOGRAFIA 34

1. INTRODUCCIÓN

El mercado del dinero está cambiando a un ritmo vertiginoso. Si hace apenas 20 años que existen las tarjetas de crédito, hoy en día los pagos realizados en efectivo están disminuyendo continuamente, sobre todo si hablamos de grandes cantidades de dinero. Las propias familias tienen sus ahorros depositados en entidades financieras y éstas a su vez destinan ese dinero a conceder créditos. La mayor parte del dinero del que disponemos apenas lo tenemos en papel y cada vez más las transacciones se realizan por medios electrónicos.

Estamos asistiendo al paso de la intranet de la información al internet del valor. Es posible transmitir información en un instante a cualquier parte del planeta como por ejemplo en un correo electrónico, en un mensaje instantáneo de whatsapp o cualquiera de otras aplicaciones similares. Es posible buscar un determinado producto en cualquier parte del planeta, planificar las próximas vacaciones, acceder a la prensa, los blogs especializados, los artículos académicos, las segundas opiniones médicas y cualquier otra cosa que nos podamos imaginar. Debido a la reciente crisis sanitaria provocada por el COVID-19 estamos comprobando como muchos de los trabajos se pueden realizar desde casa gracias a internet.

En los últimos años, y sobre todo debido a la gran crisis financiera que hemos vivido a partir del 2008, las entidades financieras se han visto obligadas a redefinir sus negocios. Debido a cambios en las costumbres y en especial, de la población más joven, muchas de ellas se vuelven innecesarias puesto que la mayoría de las transacciones que antes se hacían en la entidad ahora es posible realizarlas desde el propio hogar gracias a aplicaciones móviles y conexión a internet.

En todo este contexto, surge una nueva tecnología denominada blockchain, tan revolucionaria que es probable que cambie la forma en la que conocemos el actual mercado del dinero. Es una tecnología con un gran potencial ya que implica la eliminación de la figura del intermediario en las transacciones, en su gran mayoría entidades de crédito y, por lo tanto, se suprimen también muchos costes a él asociados. Pero no solo se puede aplicar en el campo financiero, sino que tiene muchas otras aplicaciones que se irán desarrollando a lo largo del tiempo y que más abajo citaremos. Esta tecnología surge de la mano de la primera criptomeda, el Bitcoin, que no está respaldada por ningún Estado ni entidad.

En este trabajo comenzaremos estudiando la evolución del dinero hasta llegar a lo que actualmente conocemos como dinero electrónico para posteriormente analizar el papel que hoy en día tiene la tecnología blockchain en la sociedad así como su funcionamiento. Además, hablaremos de todo lo que rodea el mundo de las criptomonedas y en especial el Bitcon, la más famosa y utilizada hasta la fecha. Por último, comentaremos también el futuro prometedor que tienen los “Smart Contracts” y las ICO.

2. HISTORIA DEL DINERO: DEL TRUEQUE A LA APARICIÓN DEL DINERO ELECTRÓNICO

El dinero, tal y como lo conocemos hoy en día, ha pasado por muchas etapas que vamos a desarrollar.

Su historia comenzó con el trueque, esto es el cambio de un bien por otro. Para poder realizar transacciones se debe tener un valor de referencia o un bien como medio de cambio. Sin embargo, este sistema tenía varios inconvenientes y al desarrollarse las sociedades se quedó obsoleto.

Para suplir esta obsolescencia apareció el dinero-mercancía, que buscaba un bien de referencia que fuera fácilmente transportable, duradero, divisible y con un valor establecido. Se trataba de un bien que tuviera el mismo valor como unidad monetaria que como mercancía y se empezaron a usar los metales preciosos, en especial, oro, plata y cobre como dinero.

Las monedas de metal comenzaron a funcionar por su facilidad de conversión y apilamiento. Además, su fiabilidad estaba fuera de toda duda y cada sociedad las acuñaba para estandarizar el comercio dentro de sus fronteras. Los europeos fueron de los primeros pueblos en elaborar monedas metálicas estandarizadas y certificadas y surge lo que se conoce como el "dinero metálico" ya que su valor venía determinado por su contenido en metales preciosos.

En la Edad Media surge el dinero en papel. La gente entregaba a los orfebres el oro del que disponían para su custodia y ellos emitían una especie de certificados para garantizar su devolución cuando se quisiese (muy parecido a lo que realizan las entidades de crédito hoy en día). La costumbre y la práctica hicieron que las compras se fueran realizando con estos certificados al ser más cómodo y seguro que ir transportando el oro, y se convirtieron en billetes de banco.

Este dinero-papel es un bien que tiene valor como medio de cambio al estar respaldado por la confianza en el emisor, que debía tener en depósito metales preciosos por un valor equivalente a lo emitido.[1]

Posteriormente entra en escena el dinero fiduciario, que a pesar de ser parecido al dinero papel, en este caso no se necesita equivalencia en metales preciosos, sino que al ser aceptado por todos genera la confianza suficiente como para ser medio de cambio. La única condición necesaria es que debe tener un respaldo, es decir, debe haber un control que es el que suelen otorgar los Estados.

En el siglo XIX surge el patrón oro, un sistema en el que el valor de cada moneda se fija en términos de una cantidad de oro concreta. Es decir, el emisor de la moneda garantiza que los billetes y monedas emitidos están respaldados por una cantidad de oro determinada. El patrón oro se mantuvo vigente en Estados Unidos hasta 1971, año en el que se decidió adoptar el dólar estadounidense como divisa internacional mediante los acuerdos de Bretton Woods. Desde ese momento, al dólar le sostuvo únicamente la confianza que hubiera depositada en él y en la economía estadounidense. A partir de entonces, en el mundo actual el dinero carece de respaldo, de valor intrínseco. Estamos

[1] https://criptomonedaonecoin.wordpress.com/2017/03/18/el-origen-y-la-evolucion-del-dinero

hablando de dinero fiat es decir, aquel dinero de curso legal cuyo valor no deriva del hecho de ser un bien físico o mercancía, sino por ser emitido y respaldado por un gobierno. [2]

Actualmente el dinero lo crea, en el caso de Europa, el Banco Central Europeo; la Reserva Federal para EEUU y los bancos centrales de cada país en el resto del mundo. La autoridad monetaria garantiza que su oferta será limitada y esto otorga confianza a los miembros de la comunidad para su uso.

Con las nuevas tecnologías surge la digitalización del dinero gracias a las tarjetas de crédito, de débito y a las cuentas bancarias. En las economías modernas la mayor parte de las transacciones no suponen un intercambio de billetes o monedas, sino que se realizan transacciones directamente entre cuentas. El dinero digital implica un intercambio distinto al físico que permite transacciones instantáneas y transferencia de propiedad sin fronteras.

Como último paso en esta evolución, en el año 2009 surgen las criptomonedas que más tarde analizaremos.

3. EL PAPEL DEL DINERO ELECTRÓNICO EN LA ECONOMÍA ACTUAL

El dinero electrónico se define como el sustitutivo electrónico de las monedas y los billetes de banco, almacenado en un soporte electrónico como, por ejemplo, una tarjeta inteligente y que, en general, está pensado para efectuar pagos electrónicos de cuantía limitada.[3]

Se puede utilizar:

1. Para realizar pagos en internet. Por ejemplo, mediante las tarjetas prepago, además de la seguridad de la que disponga el instrumento que se utilice (tarjeta, teléfono, etc), está la garantía del límite de disposición, ya que sólo se puede realizar pagos por el importe anteriormente establecido.
2. Para realizar cómodamente pequeños pagos. Al ser aceptado como medio de pago por empresas distintas al emisor, se permite pagar en autobuses, teléfonos, restaurantes, tiendas, quioscos, etc.
3. También para disponer de grandes cantidades de dinero

Según el Banco de España, “las entidades de dinero electrónico son personas jurídicas autorizadas a emitir dinero electrónico, entendiendo como tal 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 y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico. Las entidades de dinero electrónico pueden además prestar servicios de pago no relacionados con la emisión del dinero.” Sus características principales son las siguientes:

1. Son empresas que, en el ejercicio de esta actividad, no pueden recibir fondos por importe superior al valor monetario emitido.
2. Han recibido autorización para su creación del Ministerio de Economía y Hacienda, previo informe del Banco de España.
3. No pueden operar sin haber obtenido la autorización para esta actividad y sin hallarse inscrita en los registros pertinentes.

[2] https://oroinformacion.com/que-es-y-como-funciona-el-patron-oro/
[3] https://www.eleconomista.es/diccionario-de-economia/dinero-electronio

4. Están sujetas al control y la supervisión del banco de España, así como de su registro.
5. Su regulación está contenida en la Ley 21/2011, de 26 de julio de dinero electrónico, modificada por el Real Decreto-ley 19/2018, de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera, y su reglamento de desarrollo aprobado por Real Decreto 778/2012, de 4 de mayo de régimen jurídico de las entidades de dinero electrónico en la medida en que no se oponga al RD Ley 19/2018.[4]

Corresponderá al Banco de España autorizar la creación de las entidades de dinero electrónico, previo informe del Servicio ejecutivo de la Comisión de prevención del blanqueo de capitales e infracciones monetarias en los aspectos de su competencia.

En cuanto a su uso global, el dinero electrónico le está ganando la partida al dinero en efectivo ya que un estudio reciente de la Reserva Federal (Banco Central de EE UU) demostró que el efectivo representó en el año 2017 solo el 30% de las transacciones comerciales en el país; y el Informe Nielsen, que trata sobre la industria de pagos, estima que el uso de medios electrónicos de pago aumentará al 84% en comercios minoristas para 2022.

Según dicho informe, un 93% de la población europea ha realizado alguna compra online a lo largo del 2018. En el siguiente grafico podemos ver las preferencias de compra de los europeos durante dicho año, encabezando la lista los viajes con un 62%, seguido de moda y libros y música.[5]

En el año 2020, con la actual crisis provocada por el COVID-19 se está observando un brusco descenso del uso del efectivo ante la población por temor a ser una fuente de contagio. No obstante, según advierten los expertos "Si el efectivo no se acepta generalmente como medio de pago, esto podría abrir una 'brecha de pagos' entre quienes tienen acceso a pagos digitales y quienes no lo tienen.[6]

Gráfico 1. Categorías de compra online.

Fuente: Nielsen (2018) Encuesta global sobre comercio conectado.

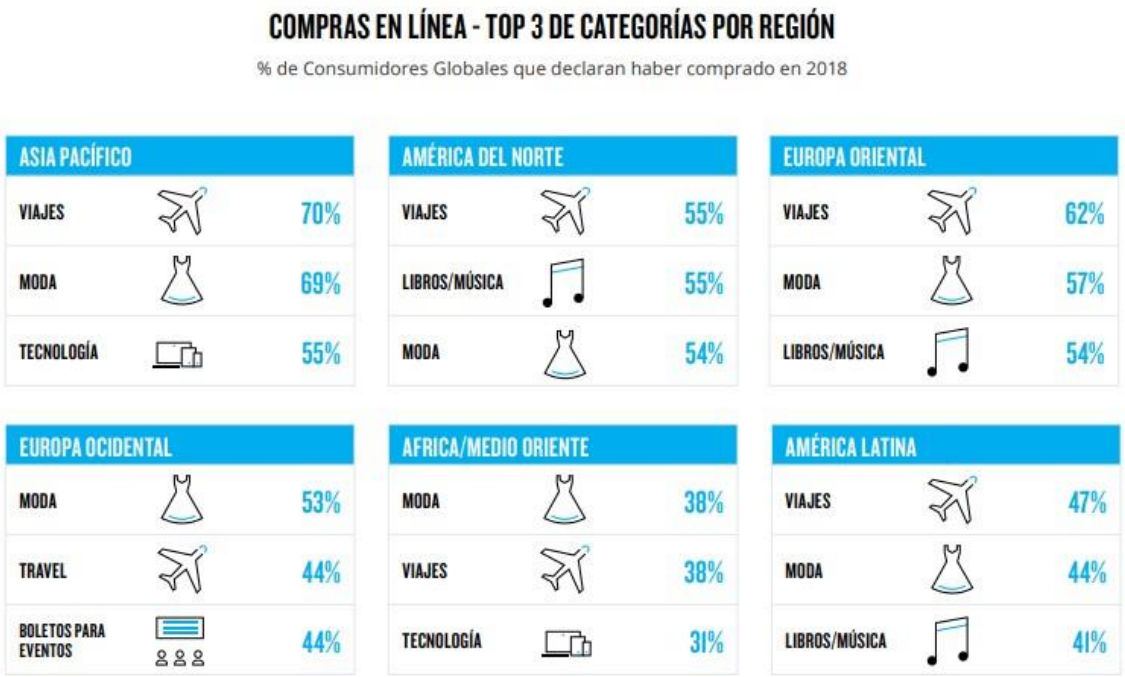
[4] Portal cliente bancario del Banco de España

[5] Encuesta global sobre comercio conectado de Nielsen 2018

[6] Vicente, N. (11 de abril de 2020). El coronavirus amenaza con poner fin al dinero en efectivo antes de lo previsto. El economista.

Si analizamos el siguiente gráfico sobre compras online por regiones, siguen dominando los viajes en la mayoría de ellas, aunque también cabe destacar el predominio de la moda. Hoy en día resulta muy cómodo comprar ropa y accesorios desde el hogar con tan solo un click en ordenador o móvil. Por otro lado, debemos resaltar que en Europa occidental se usa mucho internet para comprar entradas para eventos como conciertos, musicales o espectáculos por delante de música, libros o tecnología.

Gráfico 2: Principales compras online por regiones



Fuente: Nielsen (2018) Encuesta global sobre comercio conectado.

Por otra parte, la proporción de hogares que no usan servicios bancarios se encuentra en mínimos históricos en los países industrializados. En los EE UU, el 93,5% de los hogares tienen una cuenta bancaria, mientras que en los hogares de inmigrantes esta cifra se sitúa en el 89,9%.[7]

En el año 2009 aparece una innovación financiera cuyo potencial aún desconocemos. Surge la primera criptomoneda denominada bitcoin y la tecnología que la sustenta, la blockchain, que serán objeto de este trabajo fin de grado.

4. LA APARICION DEL BITCOIN Y LA TECNOLOGÍA ASOCIADA

La aparición de la primera criptomoneda y de la tecnología blockchain tiene lugar en el año 2008 de la mano de "Satoshi Nakamoto", el seudónimo de una persona o grupo de personas hasta ahora desconocida. Introducía el concepto en apenas nueve páginas mediante un texto denominado *"Bitcoin: a peer-to-peer electronic cash system"* a través de un foro online de criptografía.

Nakamoto es el artífice de la primera transacción de bitcoins con la que se da comienzo a toda la cadena de bloques. La blockchain es el protocolo que sirve de base a la a Bitcoin y

[7] Vivanco, F: Keller, L. (3 de mayo, 2019) Las ventajas de enviar dinero digital. El País.

en su diseño y funcionamiento es muy relevante la criptografía, que significa el uso de funciones matemáticas o algoritmos para la encriptación de la información, la opacidad de las comunicaciones.

En su escrito, Nakamoto establecía el nacimiento de "una versión puramente electrónica de efectivo que permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera".[8]

En cuanto a la persona o personas que están detrás de esta publicación pocas cosas se saben de él o ellos públicamente. La mayoría de las teorías apuntan a un matemático y criptógrafo de unos 40 años y aunque en un principio se creyó que se trataba de una persona de nacionalidad japonesa, no se llegó a confirmar ya que habla inglés perfecto. A lo largo de estos años mucha gente se ha dedicado a investigar. Sin embargo, siempre que se decía que podría tratarse de una persona conocida, el aludido lo negaba. Desde el año 2011, Satoshi no ha vuelto a publicar ningún artículo[9].

Profundizando más en el bitcoin, se trata de la primera moneda digital que surgió y la que proporcionó el sustento tecnológico que está transformando el mercado dinerario. Es una moneda descentralizada e internacional que supuso la primera aplicación exitosa de la tecnología blockchain en el ámbito económico y la primera criptomoneda.

Como ya explicamos anteriormente, surge en el año 2008 como respuesta a la gran crisis financiera que vivimos durante ese mismo año. Se trata de una propuesta revolucionaria que pretende descentralizar la economía. En el artículo original que Nakamoto presenta en la red expone las claves del sistema que estaría basado en una economía descentralizada al no estar respaldada por ningún gobierno o institución si no por aquellos que lo aceptan. Son las personas particulares las que defienden y sustentan esta nueva forma de dinero.

El bitcoin es una moneda que comenzó valiendo cero, y su valor se fue incrementando a medida que pasaba el tiempo. Una de las reglas que impulsó Nakamoto fue que únicamente puede haber 21 millones de monedas para toda la gente del mundo, esto quiere decir que se vuelve exclusiva. Cuanta más gente la quiera, más aumenta su valor.

Cualquiera puede comprar esta moneda, basta con invertir, cambiar el dinero e intercambiarlo por esta moneda digital. La creación de la misma se produce mediante la actividad de minería. Las transacciones realizadas con bitcoins se quedan grabadas en bloques; toda persona puede participar en la creación de un bloque y solo necesitará dos cosas: un poder de procesamiento de cómputo y energía eléctrica. Para crear uno de estos bloques se requiere resolver problemas matemáticos mediante gran cantidad de energía y, por lo tanto, un ordenador de uso común no es válido.

Una primera aproximación a la minería supone que la cadena o el sistema van a poner a disposición un problema matemático, y a él van a llegar todos los dispositivos conectados a la red para resolverlo. Aunque todos están trabajando para obtener la solución correcta, solo uno lo logrará y, por lo tanto, obtendrá la recompensa de un bitcoin. Conforme pasa el tiempo, la dificultad es mayor y se necesitan grandes sistemas para resolverlos.

El total de bitcoins son 21 millones y conforme el número de bitcoins emitidos se acerca a dicha cifra, el cálculo para resolver los problemas se va dificultando. Se calcula que para 2140 los bitcoins se habrán agotado. El precio cada vez será mayor, va a ser más codiciado.

[8] https://bitcoin.org/bitcoin.pdf
[9] González Meneses, M. (2017): pág. 16

Cada vez, las personas que los tengan, van a ir vendiéndolos más caros por la ley de la oferta y la demanda.[10]

Según la web criptonoticias.com se estima que más de un millón y medio de bitcoins estarían perdidos para siempre debido a varias razones, como por ejemplo recompensas no reclamadas por los mineros, transacciones erróneas o robos, pero sobretodo, en su mayoría se debe a que los compradores han olvidado la contraseña de la cartera o monedero donde los tenían guardados.[11]

5. TECNOLOGÍA BLOCKCHAIN

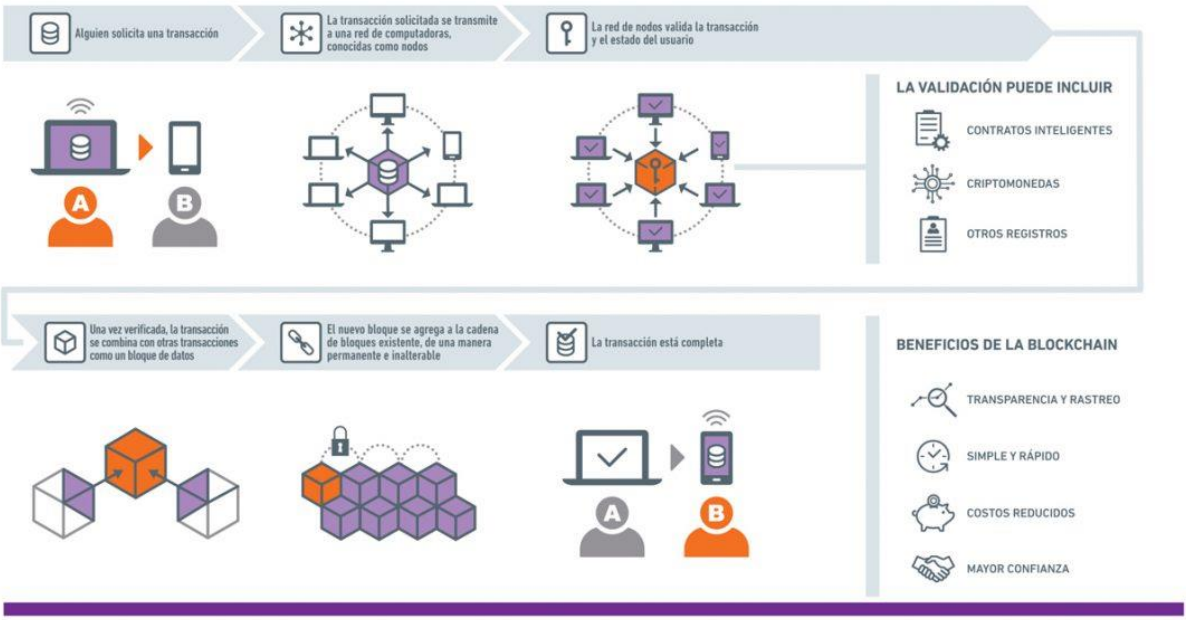
Una primera definición de blockchain, es que "se trata de una base de datos distribuida entre varios usuarios, protegida mediante criptografía y organizada en bloques de transacciones que están relacionados entre sí matemáticamente, es decir, es una base de datos descentralizada que no puede ser alterada y por lo tanto está basada en la confianza y el consenso"[12].

La blockchain supone una revolución de la tecnología descentralizada mediante una cadena de bloques. Aunque los avances tecnológicos sucedan cada día, esto supone una verdadera transformación que puede ser definida como un registro contable, inalterable y público de información. No es una tecnología totalmente nueva, sino que va agregando conceptos y métodos que ya se conocían como redes P2P o técnicas criptográficas para realizar intercambios seguros, nodos, etc.

La tecnología blockchain es como un libro mayor de contabilidad distribuido, es decir, una base de datos distribuida formada por cadenas de bloques que han sido diseñadas para no poder modificarse una vez que el dato ha sido publicado en el libro mayor o la base de datos. Quiere esto decir, que los datos son inmutables y que esta tecnología sirve para ser programada para cualquier cosa que represente valor, no solo para transacciones. Gracias a esto, podemos estar hablando del Internet del valor, al garantizar de forma descentralizada y segura las transacciones ya sea de dinero o de cualquier otra cosa, es decir, se pueden transmitir valor y confianza, cosa que hasta ahora solo lo hacían las entidades financieras[13].

[10] Domingo, C. (2018); González Meneses, M (2017)
[11] Coin Metrics' State of the Network: Issue 26 November 2019
[12] González Meneses, M. (2017) pág. 23
[13] Domingo, C. (2018) págs. 102-104

Gráfico 3. Funcionamiento de la Blockchain



Fuente: Cómo funciona Blockchain

En esta cadena de bloques vamos a poder almacenar todo tipo de información, de carácter personal, económico, contratos, etc. La gran ventaja de esta tecnología es que se trata de un registro de libre acceso para todas las personas de forma gratuita, anónima y completamente segura.

Adentrándonos en el aspecto más técnico, tenemos una cadena de bloques que podemos definir como un libro contable para registrar información que puede venir de un resultado, de un acuerdo, de un movimiento interno, etc.

Para almacenar la información vamos a necesitar una carpeta, un lugar donde guardar toda la información, y este lugar es el bloque. A su vez, el bloque tiene tres partes:

1. Por un lado, está la información que vamos a guardar, en nuestro caso, las transacciones que tuvieron lugar en un periodo de tiempo;
2. Un número de identificación personal o un conjunto de caracteres que definirá este bloque y cuyo libro contable identificará. Cada bloque tendrá un número de serie.
3. La tercera parte es el número de serie que identifica al bloque anterior, es un conector. Tenemos una secuencia de cada transacción que se va a realizar a lo largo del tiempo

A la hora de determinar el número de serie de cada bloque entra en juego la criptografía, que es lo que va a aportar gran seguridad. La criptografía coge la información de cada bloque y la encripta, la convierte en un carácter alfanumérico, esto es, un conjunto de varios números y letras que pueden parecer al azar, pero es el resultado de la criptografía aplicada a la información. Garantizamos con esto que cada bloque sea único. Si alguien intentara modificar la información de los bloques, automáticamente estaría modificando el número de identificación los bloques y ya no podría encajar ni con el anterior ni con el siguiente. Al modificar la información se modifica el resultado, el número de identificación.

La información se guarda en bloques de cadena. Partimos de un bloque inicial, el génesis, que no está anidado a ninguno anterior. Las transacciones las hacen los usuarios que

trabajan en la red. Habitualmente, si en la transacción interviene un banco, tenemos a una institución bancaria centralizada que es la encargada de llevar a cabo el control. Sin embargo, gracias a la blockchain, en la cadena de bloques cualquier persona que tenga un dispositivo con capacidad de almacenamiento y de cómputo va a poder participar en esta cadena de bloques con simplemente descargar un programa y ejecutarlo. Toda la información que se suba a esa red va a ser distribuida entre las personas que decidan participar de forma voluntaria en el proyecto. Esto genera descentralización al poder formar parte todos ella y supone ciertos beneficios, ya que la cadena de bloques tiene un elevadísimo nivel de seguridad. Solo podría sufrir un ataque cuando todas las computadoras estuvieses apagadas, lo que nunca ocurrirá. Es prácticamente imposible que se caiga el sistema.

La actividad de minar criptomonedas llegará a cambiar el sistema financiero tal y como lo conocemos, los sistemas notarial y registral y puede que hasta incluso el sistema jurídico.

Por lo tanto, como hemos, visto esa nueva revolución tiene tres partes fundamentales:

1. La criptografía: Es el procedimiento que transforma un mensaje mediante un algoritmo con una determinada clave. Si no se dispone de tal clave el mensaje será incomprensible. Es lo que dota al sistema de una gran seguridad.
2. Cadena de bloques: Base de datos que almacena todos los registros que realizan los usuarios.
3. Consenso: El protocolo común que verifica y confirma las transacciones realizadas. Los usuarios deben recibir una copia actualizable e inalterable de todas las operaciones

Uno de los aspectos fundamentales de la blockchain que sustenta al bitcoin es el uso de la tecnología P2P, ya que cada vez que se realiza una transacción se comunica al conjunto de los usuarios mediante dicha tecnología. En el caso del bitcoin, por ejemplo, se realiza a través de la aplicación informática.

Sin embargo, el mensaje no debe llegar a todos y cada uno de los usuarios de la red, sino a los conocidos como “nodos” o “mineros”, que son los usuarios que tienen un papel más relevante en el sistema y que sin ellos no podría funcionar. Cualquier persona puede convertirse en minero de bitcoin, ya que lo único que se necesita es un equipo informático con alta potencia.

Los mineros recogen todos y cada uno de los nuevos mensajes de transacciones de bitcoins que se emiten en cualquier lugar del mundo por los usuarios de esta moneda y los validan, los verifican mediante las firmas electrónicas que incorporan y la disponibilidad efectiva de esas monedas por quien los está transfiriendo. Cada minero tendrá que disponer del historial completo del sistema bitcoin para realizar el indicado cotejo.

El registro lo forman todos los mineros a la vez mediante la generación sucesiva de bloques de transacciones de la siguiente forma: cada minero recoge las transacciones que tienen lugar en el sistema, cuando dispone de unas cuantas en un determinado tiempo, forma un paquete lo que se conoce como “bloque” que debe ser incorporado al registro de Bitcoin.

La función de enlazar bloques se realiza mediante apuntadores hash, los cuales conectan el bloque actual con los anteriores y permiten su fácil verificación. En otras palabras, cada bloque está compuesto por todas las transacciones que se incluyen en él y además como primer componente está el hash del bloque anterior. A su vez el nuevo bloque calcula su

propio hash que posteriormente se incluirá como primer ítem en el siguiente bloque, y así sucesivamente. [14]

Los bloques unidos unos a otros van formando una cadena, y cada vez que se incorpora un nuevo bloque, se añade una autenticación a todo el contenido anterior de la cadena, lo que supone un aumento de la seguridad de todo el registro.

Como cada bloque integra el hash del bloque anterior, si se altera cualquier dato en un bloque alterará también el hash de ese bloque y de todos los posteriores y por lo tanto será muy fácilmente detectable.

Cada minero está trabajando con su ordenador para dar lugar al nuevo bloque de transacciones de la cadena, pero solo uno lo logrará. El contenido de los bloques que forma cada minero es diferente ya que, por un lado, las transacciones no llegan a la vez a todos y por otro lado, dentro de cada bloque se alberga una primera transacción originaria a favor del propio minero, es decir, a favor de la dirección de bitcoin de ese minero.

Para que el blockchain sea un historial único y coherente, solo se incorpora a la cadena uno de esos bloques que se están generando a la vez. ¿Cómo se selecciona este bloque? Mediante lo que se conoce como una prueba de trabajo.

La prueba de trabajo constituye un elemento esencial para la seguridad y formación de la cadena de bloques. Para cerrar un bloque, es necesario resolver un problema matemático que está relacionado con el hash del bloque.

El minero que consiga cerrar un bloque e incorporarlo a la cadena recibe un premio y es que el sistema le regala un determinado número de nuevos bitcoins. Al principio la retribución se fijó en 50 bitcoins, mientas en 2016 ya había bajado a los 12,50.

Se les denomina mineros precisamente por esto, porque como beneficiarios de estas transacciones, son los que generan e introducen los nuevos bitcoins que van incrementando la masa dineraria en circulación, como si extrajesen el metal precioso de una mina. Y es gracias a este incentivo que hay usuarios interesados en participar en esa tarea de recoger y validar las transacciones y formar con ellas los nuevos bloques que integran la cadena.[15]

De esta forma se lleva la contabilidad de las transacciones de forma distribuida sin necesidad de un tercero. Sin embargo, esto también acarrea un coste tanto de recursos informáticos como eléctricos ya que la actual complejidad de las pruebas de trabajo exigidas conlleva un elevadísimo consumo de electricidad. La prueba de trabajo desempeña una función clave para la seguridad y fiabilidad del sistema, al ser la herramienta que asegura que los bloques van a resistir cualquier intento de cambio, es decir, que no se van a poder modificar.[16]

Por último, cabe resaltar que uno de los problemas fundamentales en las transacciones financieras es el llamado problema del doble gasto. El doble gasto quiere decir que no se destine un mismo saldo a más de una disposición de personas diferentes. Para evitar este problema se recurre a un registro cronológico de transacciones que comprenda todas y cada una de las que realicen los usuarios de la moneda. Además, para dotar este registro de mayor seguridad si cabe, transacciones ya empleadas como input de una transacción, no pueden ser empleadas otra vez como input de transacciones posteriores.

[14] Guaita Martínez, J.M. (2019): Las criptomonedas: Digitalización del dinero 2.0. Pg 50
[15] Domingo, C. (2018); González Meneses, M (2017); Preukschat, A. (2017),
[16] https://bitcoin.org/es/como-funciona

5.1 BLOCKCHAIN PÚBLICA Y PRIVADA

Hay dos tipos de blockchain en función de quien pueda participar en ella. Si puede hacerlo cualquier persona estamos ante una blockchain pública, mientras que si su participación se encuentra limitada es el caso de una blockchain privada. Ninguna de ellas necesita alguna autoridad que valide los procesos.

Al principio todas las cadenas eras públicas, abiertas, descentralizadas y pseudoanónimas. Quiere esto decir que cualquier persona podía tener acceso a las transacciones y ser usuario. Todos los participantes eran iguales entre sí, y quien realiza las transacciones no podía ser identificado. No obstante, sí que es posible conocer su dirección.

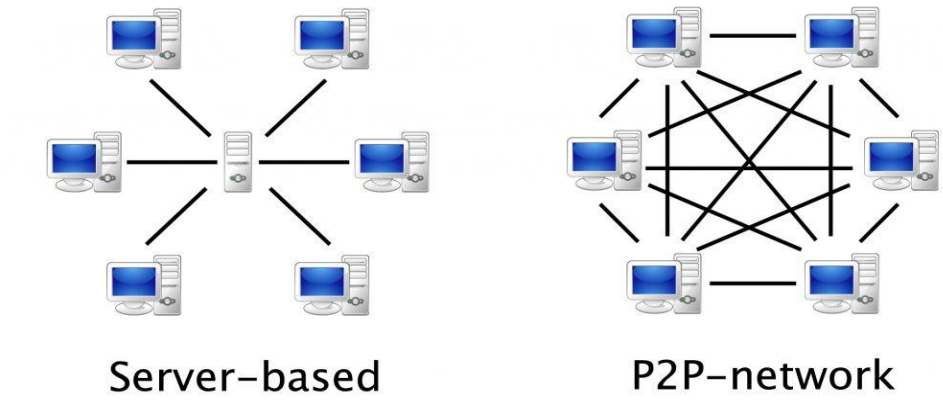
Con el paso del tiempo y ante las grandes posibilidades que se intuía podía aportar esta tecnología, fueron surgiendo las blockchains privadas que suelen ser cerradas, distribuidas y anónimas, lo que supone que solo los usuarios de la misma y los invitados a participar en ella pueden tener acceso a las transacciones realizadas. Que sean distribuidas significa que los nodos suelen estar limitados al conjunto de participantes.

5.2 ELEMENTOS BASICOS DE LA TECNOLOGIA BLOCKCHAIN Y SU SEGURIDAD

Para dar una definición más extensa, diremos que una blockchain es un conjunto de servidores a los que denominamos nodos, que utilizan un mismo sistema de comunicación conectados a una misma red y cuyo objetivo es validar y almacenar la misma información que se encuentra en una red P2P. Lo más importante y relevante es que la información contenida no se puede modificar gracias a algoritmos criptográficos. Los aspectos más importantes son los siguientes:

1. Nodo: El único requisito de la blockchain que se esté utilizando, es que todos tengan el mismo software. En la pública no se deben identificar mientras que en la privada sí.
2. Protocolo estándar: Se trata del software utilizado para que los nodos puedan comunicarse entre sí.
3. P2P, red de pares: Es la red que conecta a todos los nodos directamente.
4. Sistema descentralizado: Quien controla la red y valida las operaciones son todos los ordenadores conjuntamente conectados. En la pública no habrá jerarquía de ningún tipo mientras que en la privada puede que si la haya.

Gráfico 4. Red centralizada y red descentralizada o red P2P



Fuente https://como-funciona.com/peer-to-peer/

El bitcoin o cualquier otra moneda funcionan a través del blockchain, podemos definirla como un registro de transacciones único pero que se lleva de forma descentralizada. Se tiene en cuenta un "ledger" que es como un libro mayor de contabilidad, que es llevado por todos los usuarios a la vez.

La cadena de bloques es un registro único, unitario, pero de alcance y contenido universal: en ella están registradas todas las transacciones de bitcoins que se han llevado a cabo en todo el mundo desde que se creó el primer bitcoin. Este registro se genera en la red y es guardado en los discos duros de los ordenadores que forman parte del sistema. Para controlar este registro no hace falta ninguna autoridad ni tercero de confianza, es la propia red la que es segura.

La fiabilidad del sistema, se basa en dos tipos de algoritmos matemáticos: algoritmos de encriptación asimétrica o de doble clave y algoritmos de resumen o "hashing".

La autentificación de los mensajes de transferencia se basa en firmas electrónicas de doble clave. A cada usuario del sistema se le asignan dos claves de encriptación, que están matemáticamente enlazadas, de manera que lo que se encripta con una se desencripta con la otra y viceversa, por lo tanto, el conocimiento de una de las claves no sirve para deducir la otra clave y esto es lo que permite utilizar una de las claves como privada y la otra como pública. Esto a su vez hace que el desarrollo de las comunicaciones entre desconocidos sea seguro.

La finalidad de esta herramienta de encriptación es el aseguramiento de la procedencia de una comunicación para el destinatario de ésta.

Se necesitan dos requisitos para que el sistema sea completamente seguro:

1. El registro de claves públicas debe ser fiable, por lo que los procedimientos mediante los cuales se imputa o atribuye a una persona una clave pública, deben ser seguros y el registro debe mantenerse en todo momento accesible y actualizado.
2. El usuario debe tener cuidado con su clave privada y guardarla adecuadamente.

Al utilizar blockchain, el sistema de claves es completamente descentralizado, es decir, no existe ninguna autoridad o entidad de certificación de la clave pública asociada a una persona determinada. No importa quién es la persona que ha registrado una determinada clave pública y por tanto que puede utilizar la correlativa clave privada (Domingo, 2018).

6. CRIPTOMONEDAS: ASPECTOS GENERALES

La aparición del bitcoin en el año 2009 sentó las bases para el surgimiento de nuevas criptomonedas lo que sin duda es una revolución en el campo de la economía de consecuencias aún impredecibles. Dedicaremos este epígrafe a explicar las características generales de las criptomonedas y su funcionamiento.

Se definen las criptomonedas como una especie de moneda virtual, que puede ser intercambiada y operada como cualquier otra divisa tradicional, pero que queda al margen de los gobiernos e instituciones financieras. [17]

[17] https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas

Según el BCE (Banco Central Europeo) una moneda virtual es un "tipo de dinero no regulado, digital, que se emite y por lo general controlado por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual especifica." Es decir, es dinero en sentido económico, pero no es dinero en sentido jurídico.

En palabras de Andrei Boar (2018) también se puede definir como un activo que se crea fuera del sistema financiero tradicional, basado en la confianza y en la aceptación de los usuarios a través de un sistema criptográfico gracias al que podemos realizar transacciones dinerarias entre los miembros de la comunidad.

Son monedas "peer to peer" y distribuidas que los usuarios pueden usar para lo mismo que usan el dinero fiduciario [18]: comprar o vender bienes, enviar dinero a otras personas u organizaciones o extender un crédito. Las criptomonedas pueden ser vendidas o compradas en centros de intercambios denominados exchanges. Además, son la forma perfecta de dinero para internet porque son rápidas, seguras y no tienen fronteras.

Se trata de monedas completamente virtuales, no existen monedas físicas, de hecho, ni siquiera existen en formato digital tampoco. Las monedas, o los balances de cada usuario, son obtenidos a partir de la suma de todas las transacciones. Los usuarios tienen las claves privadas que les permiten tener acceso a los fondos de una cartera y si la pierden u olvidan jamás podrán volver a acceder a ellos. La posesión de un par de claves públicas y privadas es el único requisito a la hora de utilizar una red de criptomonedas.

Siguiendo a Navas (2015), como características principales debemos destacar[19]:

1. No poseen representación física
2. Son descentralizadas, lo que supone que no están bajo el control de ninguna entidad financiera o estado
3. Se trata de monedas internacionales
4. Son anónimas por lo que las transacciones se realizan de forma anónima
5. No se necesitan intermediarios;
6. Tienen una función aceleradora ya que otorgan agilidad a los intercambios y a las operaciones de pago.

Bitcoin fue la primera criptomoneda, pero a partir de ese momento comenzaron a surgir muchas más hasta el día de hoy que se calcula que hay sobre 2500 aunque éxito tienen pocas. Se utilizan otros algoritmos y se les dota de otras propiedades aunque siguen teniendo el uso de la red P2P descentralizada, inmutabilidad y transacción electrónica segura[20].

Mediante la siguiente tabla vamos a definir los rasgos y las principales características de las doce criptodivisas más populares:

[18] Dinero Fiduciario: es el que se basa en la confianza de la comunidad, de quien lo emite. Es el caso del dólar o el euro.

[19] NAVAS NAVARRO, S. (2015): "Un mercado financiero floreciente: el del dinero virtual no regulado (especial atención a los BITCOINS)", en Revista CESCO de Derecho de Consumo, núm. 13, p. 11.

[20] Domingo, C. (2018)

Tabla 1. Principales criptomonedas

Critomoneda	Código	Año	Características
Bitcoin	BTC	2009	La primera y más popular. Medio de pago descentralizado
Ethereum	ETH	2014	Mucho más que una criptomoneda. Plataforma de desarrollo de Smart Contract
Ripple	XRP	2008	Red de pagos digitales transfronterizos. Bancos y proveedores de servicios de pagos
Bitcoin Cash	BCH	2017	Escisión de BTC. 8 veces capacidad transaccional BTC
EOS	EOS	2014	Nace a través de una ICO. Descentralización tecnología vía blockchain
Litecoin	LTC	2011	Alternativa a BTC. Más eficiente y accesible
Cardano	ADA	2015	Blockchain con filosofía científica. Plataforma de desarrollo Smart Contract
TRON	TRX	2017	Origen Chino. Plataforma de entretenimiento digital.
NEO	NEO	2017	ETH Chino. Código abierto sin ánimo de lucro
DASH	DASH	2014	Dinero privado de internet con plataforma muy versátil
MONERO	XMR	2014	Asociada a la "deep web" por su casi imposible trazabilidad
IOTA	MIOTA	2014	Criptodivisa del internet de las cosas. Tangle como alternativa a blockchain

Fuente: Guaita Martínez, J.M. (2019): Las criptomonedas: Digitalización del dinero 2.0

Todas son diferentes y con usos distintos, pero tienen un procedimiento en común pues la creación de la mayoría de las criptomonedas tiene lugar gracias a las actividades de minería que más tarde desarrollaremos. Como resumen, se trata de verificar los bloques enviados por los usuarios y al mismo tiempo resolver los problemas matemáticos que se plantean para crear la blockchain. El primer minero que solucione el algoritmo recibe un premio en forma de criptomoneda, pero puede decidir si la guarda o la convierte en dinero fiduciario. No obstante, solo algunas monedas, las más conocidas pueden ser cambiadas directamente a euros o dólares.[21]

Por orden de capitalización, las principales criptomonedas son actualmente el Bitcoin, Ethereum, XRP, Tether, Bitcoin Cash, Bitcoin SV, y Litecoin. [22]

6.1 ¿CÓMO SE COMPRA O SE INVIERTE EN CRIPTOMONEDAS?

Actualmente en el mercado existen tres formas diferentes de comprar o invertir en criptomonedas:

1. Exchanges: Es una especie de casa de cambio donde se pueden comprar y vender criptomonedas. Es el modo más sencillo. Hay varios tipos:
    - Casa de cambio "bróker": la empresa o casa de cambio es quien compra las criptomonedas y posteriormente las vende a los usuarios con alguna comisión. Es la opción más sencilla pero también la más cara.
    - Casa de cambio "tradicional": son las más populares. Se trata de exchanges que ofrecen una plataforma de trading en la que los usuarios intercambian

[21] Boar, A. (2018); pag. 19
[22] https://coinmarketcap.com/es/

criptomonedas libremente a precio de mercado. También cobran comisiones por cada transacción.
    - Intercambios P2P: ofrecen el intercambio “peer to peer”, es decir, unas criptomonedas por otras.
2. Intercambio de bienes y servicios y como contraprestación se reciben criptomonedas. Se trata de empresas que pagan a sus empleados principalmente en Bitcoins.
3. Minería: mediante una prueba de trabajo se minan bloques en blockchain para conseguir las criptomonedas. [23]

6.2 REGULACIÓN LEGAL

Actualmente no encontramos legislación específica contable o fiscal que regule el uso de las criptomonedas, pero esto no significa que el usuario no esté obligado a realizar sus obligaciones fiscales en los diferentes impuestos que se vean afectados ya que si la cantidad defraudada supera los 120.000 € el sujeto puede estar cometiendo un delito fiscal contra la Hacienda Pública.[24] Ante las dudas que surgen en los usuarios de las mismas, la Dirección General de Tributos, dependiente del Ministerio de Hacienda está aplicando preceptos por analogía respecto de otras figuras tributarias que están presentes en nuestro Ordenamiento Jurídico.

En ausencia de normas concretas, respecto a la fiscalidad, la mayoría de países someten a los usuarios de las mismas a alguna categoría de los grandes impuestos:

1. IRPF: El impuesto sobre la renta se aplica a todas las entidades no incorporadas que reciben bitcoins u otras criptomonedas como ingresos.
2. El impuesto de sociedades se aplica a las operaciones de ámbito empresarial importantes y que, por tanto, ocupan grandes cantidades de dinero.

Según la Autoridad Bancaria Europea, ABE, se definen las monedas virtuales como “una representación digital de valor no emitida por un banco central ni por autoridad pública ni necesariamente asociada a moneda fiduciaria pero aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos”;

Al no haber una entidad central que respalde la emisión de las criptomonedas no se consideran todavía que se traten de dinero electrónico de curso legal. No obstante, como se consideran monedas electrónicas con unidad de cuenta sí que pueden ser utilizadas como medio de pago entre sus usuarios. González Meneses, M. (2017)

Debemos destacar que existe una necesidad de elaborar y aprobar una normativa específica que regule la emisión, el almacenamiento, la propiedad y la transmisión de las criptomonedas en nuestro país.

7. ASPECTOS PRÁCTICOS EN EL USO DEL BITCOIN

7.1 CARACTERISTICAS PRINCIPALES DEL BITCOIN

“El bitcoin es una moneda virtual e intangible (criptodivisa) nacida en 2009. El término se aplica también al protocolo y a la red P2P que lo sustenta. Generalmente se usa 'Bitcoin', en

[23] González Meneses, M. (2017)
[24] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Art. 305

mayúscula, para referirse a la red o al protocolo y 'bitcoin' (plural: 'bitcoins') para referirse a las unidades monetarias."[25]

Como rasgos caracterizadores de esta criptomoneda se deben destacar los siguientes:

1. Descentralizada, lo que significa que ningún banco, institución financiera, Estado o empresa pueden controlarla. Esto supone una gran ventaja ya que no va a ser posible generar inflación al crear más moneda, sino que es la propia red a través del proceso de minería la que gestiona la emisión de las mismas de forma descentralizada y siempre en función de la demanda real. La emisión de bitcoins viene determinada por una rutina matemática preestablecida, con un calendario prefijado. Así, se generan y distribuyen de forma aleatoria, a razón de unas 6 veces por hora, lo que se denomina lotes de bitcoins; cada lote acumula una cantidad no superior a 50 bitcoins, y el tamaño del lote disminuye progresivamente, según una regla predeterminada, hasta alcanzar en el año 2140 un monto total de las monedas en circulación que no llegue a exceder los 21 millones de unidades.
2. Imposible de falsificar o duplicar: esto resulta gracias al sistema criptográfico que protege a los usuarios y simplifica las transacciones. Además de la propia red segura, la mayoría de los usuarios cuentan con sus propios monederos que suelen estar protegidos por ellos mismos.
3. Directa: en el sistema de pagos mediante bitcoin no hay intermediarios ya que las transacciones se realizan "peer-to-peer" (es decir, directamente de persona a persona) de manera instantánea y con unos costes muy bajos de procesamiento, sin necesidad de acudir a un Banco u organización que se encargue de dicha transacción.
4. Irreversibilidad de transacciones: Una vez realizado un pago, no se puede anular. En todo caso, el receptor de la moneda podría realizar una transacción de vuelta al emisor.
5. Posibilidad de cambio a euros o a otras divisas y viceversa.
6. Privacidad: en ningún momento la persona que esté utilizando bitcoins debe revelar su identidad.
7. Propiedad total: todo el dinero que se tenga en bitcoins no puede ser intervenido por las autoridades ni las cuentas pueden ser congeladas. [26]

7.2 EL PRECIO DEL BITCOIN

El precio del bitcoin no viene establecido de antemano, sino que está basado en la confianza y el uso que le den los usuarios y se determina a partir de la oferta y la demanda y por lo tanto cuanta más gente esté dispuesta a usarlo, más se elevará su precio. No hay un precio oficial para el mismo debido a que existen diversas plataformas en las que se negocian.

Desde que fuera lanzado bitcoin en enero del 2009, el precio ha variado mucho. Desde el año 2011 al 2013 apenas sufrió variaciones según podemos observar en el gráfico de abajo. Por ejemplo, a principios del 2013, el precio de bitcoin era de 25 euros mientras que al finalizar dicho año su precio había aumentado a cerca de 1000 euros.

[25] Fuente: El economista
[26] Fuente: https://blog.unimooc.com/bitcoin-definicion-caracteristicas/

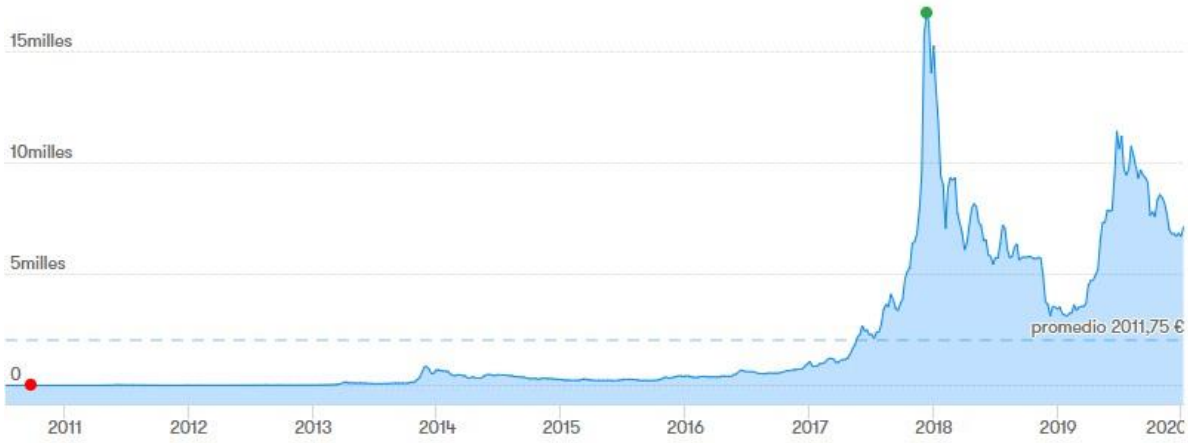
Esta senda alcista se rompe en el año 2014, cuando el mercado fue duramente afectado por la bancarrota de Mt. Gox, la primera y más grande bolsa bitcoin de ese momento.

Un año después, la casa de cambio de cambio líder europea Bitstamp fue hackeada y 19.000 bitcoins desaparecieron. Los reportes negativos como estos causaron que el precio del bitcoin se reduzca rápidamente. En enero del 2015, el precio se remontó a 180 euros.

Para el 2017, el bitcoin escaló nuevamente y alcanzó el precio de 1.000 euros. El segundo semestre del 2017 llamó la atención en los medios y ello trajo un crecimiento exponencial en el precio, alcanzando su precio histórico de todos los tiempos en diciembre por un valor de 16.727,68 euros.

Después de este gran pico y hasta la actualidad, el precio se ha caracterizado por grandes fluctuaciones.

Gráfico 5. Evolución histórica del precio del Bitcoin.



Fuente: https://www.etoro.com/

7.3 LA ADQUISICION DE BITCOINS

En la actualidad podemos distinguir tres formas de adquirir Bitcoins:

1. Mediante casas de intercambio a partir de moneda de curso legal.
2. Por recepción de una transferencia de bitcoins
3. Mediante la actividad de la minería: el proceso de creación del Bitcoin.

Para los pequeños usuarios, la mejor forma de obtener bitcoins es a través de las casas de intercambio y los monederos. Hay muchas empresas que cumplen con estas dos funciones, como si fueran entidades de crédito. Hay dos tipos de casa de cambio, las primeras nos permiten cambiar dólares o euros por criptomonedas mientras que las segundas sirven para cambiar una criptomoneda por otra.

Las casas de cambio son plataformas mixtas que permiten depositar los bitcoins de forma online y que a cambio nos piden la identificación personal y fiscal para la prevención del blanqueo de capitales.

Estas plataformas en realidad son un tercero, un intermediario en las relaciones con Bitcoins y por lo tanto podemos calificarlo como una desventaja. Por un lado, mediante las operaciones obtienen beneficio, y por otro hay riesgo de fraude y ataques. Son empresas y como tal siempre van a buscar maximizar su beneficio.

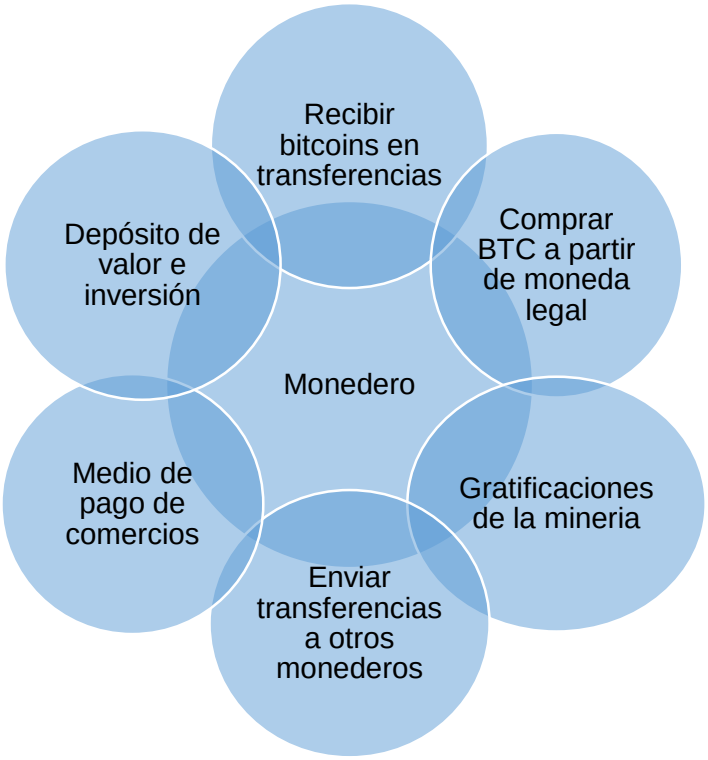
La adquisición de bitcoins mediante la actividad de minería no es asequible para los pequeños usuarios ya que consume gran cantidad de energía, el equivalente al de una familia media durante un mes, además que requiere una gran infraestructura informática. Con el paso del tiempo, la energía necesaria ira en aumento al aumentar el número de personas minando.

Mediante la recepción de transacciones también se puede conseguir Bitcoins de dos modos, o bien como donación o bien como contraprestación por los servicios prestados. Para realizar dicha transacción solo se necesita conocer la combinación alfanumérica del destinatario y a través del software o plataformas intermedias introducir la orden para mover el capital. [27]

7.4 ASPECTOS PRÁCTICOS EN EL USO DEL BITCOIN: EL MONEDERO DIGITAL

Para poder hacer uso del Bitcoin es necesario disponer de un monedero que realice las siguientes funciones:

Gráfico 6: Funciones del monedero



Fuente: Elaboración propia.

El monedero tiene la función esencial de guardar las criptomonedas aunque en realidad lo que se guarda en él es una clave alfanumérica que permite acceder al sistema para consultar las transacciones en el libro mayor. Si se pierden las claves se pierden los bitcoins. Es el primer paso para utilizar esta criptomoneda al permitir recibir, almacenar o gastarlos. Un monedero puede ser una aplicación, un sitio web o un dispositivo que se encarga de administrar las claves privadas para el usuario.

[27] Boar, A. (2018): Descubriendo el Bitcoin.

No hay que olvidar que el bitcoin es una moneda totalmente virtual y, por lo tanto, no se encuentra en formato físico ni papel.

Por un lado, existen plataformas mixtas que permiten comprar a partir de euros o dólares y guardar los bitcoins, y también existen plataformas online que solo actúa como monedero. Cabe diferenciar los monederos entre los “hot wallet” y “cold wallet”. Los primeros están continuamente conectados a la red mientras que los segundos no, y por lo tanto suponen una especie de caja fuerte. Por ejemplo, si alguien quisiese atacar nuestro monedero solo podría en caso de que tuviéramos un “hot wallet” ya que a los “cold wallet” sería imposible acceder.

Vamos a realizar una clasificación de los distintos tipos de monedero:

1. Escritorio: se trata de programas informáticos para guardar bitcoins mediante el almacenamiento de claves privadas en el ordenador, independientemente del sistema operativo del mismo. Permiten enviar y recibir bitcoins entre distintos usuarios a través de las claves necesarias.
2. Móvil o app: en este caso son aplicaciones disponibles en los móviles a través de las que podemos realizar y controlar pagos a usuarios y comerciantes a la vez que guardar nuestros propios bitcoins. Para garantizar la seguridad de las transacciones se recomienda el uso de las plataformas que cuenten con autentificación en dos pasos gracias a claves de acceso tanto personal como las enviadas al propio móvil y así cerciorarse en la identidad de quien realiza la transacción.
3. Web: son los monederos a los que podemos acceder a través de un navegador. Aunque disponen de la autentificación en dos pasos suelen usar sus propios servidores para guardar las claves de los bitcoins y, por lo tanto, pueden sufrir ataques externos.
4. Hardware: es un monedero físico y cuya ventaja reside en que permiten guardar las claves de forma desconectada de la red mediante USB o disco duro. Para realizar cualquier operación simplemente se conecta a la red y estaría listo. El software es quien carga, valida y permite realizar las transacciones mientras que las claves se encuentran en el dispositivo externo. Este sistema está libre de cualquier ataque informático pero no está libre de que nos lo pueden robar. La mayoría de personas que cuentan con él lo tienen guardado en una caja fuerte.

   Como contrapartida hay que pagar un precio de entre 20 y 120 euros para adquirirlo.
5. Paper wallet online o monederos en papel: es un método físico que a la vez puede ser complementario de los anteriores. Los usuarios de este tipo de monedero suelen crean una “cold wallet” en formato papel que es totalmente segura.
6. Paper wallet ATM: es la forma de conseguir bitcoins a través de cajeros automáticos. Actualmente en España hay más de 7000 cajeros que permiten comprar y vender bitcoins.
7. Brain wallet o monederos en la memoria: es el método más fiable y a la vez más arriesgado pues solo sirve para aquellas personas que sean capaces de memorizarse los caracteres alfanuméricos de las claves que son entre 25 y 36. Si la persona quedase incapacitada intelectualmente o falleciera los bitcoins se perderían para siempre.

Para la mayor seguridad de los monederos es necesario tenerlos permanentemente actualizados, ya que las plataformas están continuamente mejorando su seguridad.[28]

7.5 COMO ACCEDER A LA COMUNIDAD BITCOIN

Para formar parte hay que seguir una serie de pasos. En primer lugar, el registro se hace de forma privada descargándose la aplicación correspondiente en cualquier ordenador. Una vez descargada debemos hacer click en la pestaña "nueva dirección" que generará un número de 256 bits como clave privada de encriptación. A su vez, se genera otro número como clave pública del que se calcula el "hash" lo que opera como dirección Bitcoin y que en realidad es una sucesión de letras y números. En ningún momento se pide la identificación de la persona ni DNI.

El bitcoin puede funcionar como "dinero al portador" por el anonimato que este algoritmo permite. Todas las transacciones están registradas y son perfectamente trazables o rastreables, pero se producen entre simples claves públicas de encriptación. Si se quiere transmitir bitcoins a otra persona, el titular de una clave pública transfiere la cantidad que quiera al titular de otra clave pública. Solo se podrá disponer de los Bitcoins mientras se conserve la clave privada vinculada a la clave pública beneficiaria de transacciones anteriores. Perder u olvidar la clave es lo mismo que perder u olvidar el dinero ya que no se puede gastar sin la clave. Como contrapartida, si yo comunico mi clave a otra persona esta puede disponer de mi dinero. [29]

Los saldos que se tengan en Bitcoins van a ser incoercibles o inembargables. Ninguna autoridad pública puede ordenar una transferencia de fondos en esta moneda a ningún destino determinado sin contar con la voluntad del sujeto, pues solo este conocerá la clave y no se le puede obligar a que la confiese.

Las criptomonedas solo estarán disponibles para aquellas personas que conozcan la clave criptográfica privada vinculada a la clave pública del beneficiario de una transacción anterior.

En 2013, en nuestro país ha tenido lugar la incautación por parte de la policía de bitcoins en el marco de la "operación Ramson" y solo fue posible porque la policía irrumpió por sorpresa en casa de los detenidos y los pilló in fraganti con el ordenador y todas las claves disponibles. Para ello, transfirieron los bitcoins desde sus direcciones hasta una dirección de la propia policía. [30]

7.5.1. Algoritmos de Hashing

El cálculo de "hashes" es la pieza técnica clave para toda la seguridad jurídica de internet, siendo la base última de blockchain y, por lo tanto, también de Bitcoin. La función hash es un algoritmo matemático que, aplicado sobre un archivo o ítem digital cualquiera da como resultado una determinada secuencia de aproximadamente treinta caracteres alfanuméricos, es decir, letras y números.

El hash sirve para garantizar que un determinado archivo no ha sido alterado, por lo tanto, permite detectar la alteración y acreditar la que no ha existido.

Este determinado hash, cumple una función esencial en el blockchain, pues este se compone de una cadena de hashes. Cuando se desea realizar una transferencia de Bitcoins disponemos de un input y un output.

[28] Boar, A. (2018): "Descubriendo el Bitcoin",
[29] González Meneses, M (2017)
[30] Fuente: https://www.elmundo.es/elmundo/2013/02/14/navegante/1360826212.html

Como inputs disponemos del hash de la trasferencia previa, de la que resulta el saldo disponible, la firma electrónica con la clave privada del transferente y también la clave pública del mismo.

Como outputs se encuentran la cantidad de bitcoins que ahora se transfieren y la dirección de Bitcoin del beneficiario.

A la par de todo este mensaje de transferencia, se calcula su hash que es lo que sirve para identificar esta concreta transferencia. [31]

7.6. SEGURIDAD Y RIESGOS

El bitcoin es un sistema totalmente seguro, el problema es que al añadir intermediarios al realizar las transacciones se vuelve vulnerable. El sistema blockchain es infranqueable y falsificar movimientos dentro de él imposible, pero si se dispone de un monedero online o plataforma de compraventa sí que se pueden sufrir robos o ser atacados.

Lo más importante a la hora de prevenir estos ataques es tener las aplicaciones plenamente actualizadas, y guardar en las "hot wallet" la menor cantidad de bitcoins posibles. Por último, hay que asegurarse que la plataforma que estamos utilizando es realmente la empresa y no alguien que la pretende suplantar.

En cuanto a los riesgos podemos encontrar los siguientes:

1. Financiación de actividades ilícitas y/o blanqueo de capitales: La descentralización del sistema implica que las transferencias se realicen directamente entre ordenante y beneficiario ambos anónimos, sin necesidad de un administrador o intermediario. Esto supone que la identificación es altamente compleja ante posibles comportamientos sospechosos de actividades ilícitas.
2. Necesidad de elevada capacidad computacional: Aunque en principio cualquier ordenador puede participar del proceso de creación de nuevas unidades de bitcoins, se requiere una elevada capacidad computacional que se traduce en la realidad en una actividad dominada por un pequeño grupo de computadoras, con mejores conocimientos técnicos y mayor inversión en recursos informáticos.
3. Irreversibilidad de los pagos: Las transacciones bitcoin no se pueden revertir, sólo pueden ser reembolsadas por la persona que recibe el pago, es decir, la única manera de recuperar la inversión es que el que la reciba se la devuelva al emisor. Consecuentemente, debe ponerse especial cuidado en hacer negocios con personas u organizaciones de confianza o con buena reputación, de lo contrario no se podrá recuperar el dinero depositado.
4. Posibles transacciones fraudulentas: Este riesgo surge porque los protocolos sobre los que se desarrolla el bitcoin son de software abierto, aunque la implementación de sus diferentes versiones no tiene por qué producirse de manera uniforme entre todos los usuarios. Asimismo, y a pesar de las mejoras en materia de seguridad, el robo de unidades monetarias ha sido recurrente en diferentes plataformas de negociación de bitcoins.
5. Impacto sobre la estabilidad de los precios y sobre la estabilidad financiera: Las plataformas de negociación privadas en las que se pueden canjear bitcoins por monedas de curso legal tienen una gran volatilidad en las cotizaciones debido a movimientos especulativos. A esto hay que sumar que como no se garantiza legalmente la convertibilidad de estas unidades monetarias, la confianza de los

[31] González Meneses, M. (2017); páginas 75 a 80.

usuarios en el valor de la moneda depende, fundamentalmente, de sus expectativas futuras así como de la credibilidad en la solvencia técnica del esquema.

6. Garantías de privacidad: Partiendo de la base de que Bitcoin depende de que sus usuarios gestionen adecuadamente su criptografía, resulta que la gestión de claves es básicamente inservible para el usuario final, lo que acaba en una falta de usabilidad. Esta situación ha generado una serie de servicios ofertados por empresas, en principio fiables, que "poseen" las claves privadas de sus clientes. Esto claramente limita la libertad del usuario pero puede ser peor, como ya se ha puesto de manifiesto con algunos servicios que han violado las expectativas de sus usuarios.[32]

8. LOS SMART CONTRACTS LIGADOS A ETHEREUM

Una nueva plataforma pública llamada Ethereum nace en el año 2014 de la mano de un joven ruso, Vitalik Buterin y tiene como base la tecnología del bitcoin pero permite nuevas posibilidades. Su objetivo era desarrollar aplicaciones totalmente descentralizadas, es decir, que fuera la red en sí misma, la que ejecutara y validara la aplicación, la entrada y la salida y le llegara a quien estaba al otro lado sin que hubiera un punto centralizado que tomase la decisión de como ejecutar dicha aplicación. Domingo, C. (2018)

El hito más importante del Ethereum son los llamados "Smart contracts" o contratos inteligentes. Es un programa de software que se ejecuta normalmente junto con una transacción financiera. En términos coloquiales, es un tipo de programa que dice "si pasa A entonces haz B" y normalmente A es algún tipo de evento y B un pago. Es una aplicación de ejecuta las transacciones tal cual están programadas, no hay forma de modificarlas, eliminarlas o falsearlas.

Según la web oficial wwww.ethereum.org, esta plataforma permite:

- Designar y crear tu propia criptomoneda
- Crear un proyecto basado en la confianza de terceros
- Crear una organización democrática autónoma
- Crear un nuevo proyecto descentralizado

Cuenta con su propia moneda, el Ether (ETH) que es lo que se mina para que haya un incentivo económico y formar parte de la red. El Ether es la criptomoneda del sistema Ethereum. Es el principal rival del Bitcoin dentro de este mundo y para muchos posee un sistema mejorado.

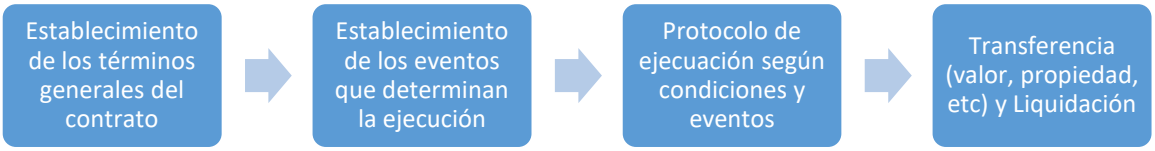
En el artículo 957 del Código Civil se establece la definición de contrato: "Contrato es el acto jurídico mediante el cual dos o más partes manifiestan su consentimiento para crear, regular, modificar, transferir o extinguir relaciones jurídicas patrimoniales". Son requisitos esenciales el consentimiento de las dos partes, y tiene fuerza de ley entre las partes. En el caso de que alguna parte decida no cumplir debe intervenir el derecho y aplicar las consecuencias jurídicas determinadas.

En el caso de los "Smart contracts" la aplicación de los mismos es automática y directa según lo acordado por las partes y no se necesita en ningún momento la intervención de un tercero para validar si se han cumplido las claúsulas, con el ahorro de costes y tiempo que eso conlleva. Otra diferencia es que no se trata de un contrato en papel, sino que existe digitalmente en la cadena de bloques, están escritos en un lenguaje de programación. En el

[32] Pacheco Jimenez, Mª N: "Criptodivisas: del bitcoin al MUFG. El potencial de la tecnología blockchain" en Revista CESCO de Derecho de Consumo, núm. 19, 2016, p. 11.

futuro, estos contratos irán mucho más allá y se convertirán en un asistente virtual inteligente que puede llegar a regular muchas cosas, aunque por el momento se trata de una tecnología que está en desarrollo.

Gráfico 7: Esquema básico de Smart Contract



Fuente: Elaboración propia

Esta aplicación de la Blockchain significa que el contrato es público, imposible de eliminar, de cumplimiento automático y sin ninguna autoridad.

Al ejecutarse en la cadena de bloques, el contrato inteligente se convierte en un programa de operación propia que se ejecuta automáticamente cuando se cumplen las condiciones específicas. Los contratos se ejecutan exactamente como fueron programados y pueden ser financieros, de compraventa, seguros, pólizas, etc. [33]

Algunos de los sectores que se verían beneficiados con su aplicación serían la banca o los seguros que a continuación desarrollaremos.

9. APLICACIONES DE LA TECNOLOGIA BLOCKCHAIN

La gran aplicación con la que surge esta nueva tecnología es la posibilidad de compartir y gestionar el valor de activos o bienes digitales, sin la necesidad de depender de una entidad central de confianza que avale todo el proceso.

Es el paso hacia el internet del valor, y las grandes ciudades del mundo ya han tomado partido. Como ejemplo de ello, en el Reino Unido se está subvencionando con una importante suma de dinero a todos aquellos proyectos relacionados con la blockchain.

En Suiza nos encontramos una zona denominada Crypto Valley con bajos impuestos para atraer las inversiones además de leyes que protegen a los emprendedores, y en EEUU también se les está dando mucho protagonismo.

Actualmente somos conscientes de cómo el internet de la información nos ha cambiado la vida, gracias a esto, podemos estar informados en cualquier instante de todo lo que acontece en el mundo, podemos comprar cualquier objeto desde el sofá de nuestra casa y a los pocos días tenerlo, e incluso podemos comunicarnos con quien queramos por muy lejos que se encuentre. El paso hacia el internet del valor traerá consigo tantas otras novedades, pues ya desde hace unos años es posible compartir valor de forma descentralizada, sin necesidad de ningún intermediario. Es una verdadera revolución. Por poner un ejemplo, hoy en día, para la compraventa de un inmueble es necesario por un lado la transferencia de dinero y por otro, elevar el contrato a escritura pública ante notario y sin embargo, si se aplicase la tecnología blockchain se podría modificar el registro de propiedad sin acudir al notario. Preukschat, A. (2017)

[33] https://blockgeeks.com/guides/es/que-es-ethereum

9.1 BANCA

El bitcoin trajo consigo una verdadera revolución al demostrar que no era necesaria ninguna entidad central para desarrollar las tareas que normalmente le corresponderían a la banca como los pagos, las transferencias o las remesas.

Ahora nos vamos a centrar en analizar las diferencias entre el sistema de pagos establecido por los bancos y el que se da con la tecnología blockchain que utilizan el bitcoin o las demás criptomonedas.

El dinero digital no es lo mismo que el bitcoin o cualquier otra moneda. Con el dinero digital llevamos ya muchos años y la mayor parte del que poseemos se denomina así. Se trata de anotaciones en cuenta, no de dinero físico o material. La mayor parte de nuestro dinero en cuenta, no se encuentra en un depósito a una cantidad equivalente en dinero físico, sino que procede de transferencias desde otras cuentas bancarias.

La gran parte del dinero que utilizamos solo tiene consistencia contable lo que le aporta garantía, además que la mayoría de los pagos que hacemos no implican circulación ni entrega física de dinero, sino que se realizan mediante órdenes de transferencia, entrega de cheques o domiciliaciones. Esto supone una gran intervención bancaria en el sistema monetario vigente lo que acarrea un coste económico para los usuarios.

El principal problema que posee el sistema financiero tradicional es la presencia de un tercero intermediario para controlar lo que sucede en todo momento y dotar de confianza al sistema. En estos casos, cuando se quiere realizar una transferencia, el cliente da la orden al banco en el que tiene depositados sus ahorros. La entidad tendrá que realizar una serie de comprobaciones; en primer lugar, debe verificar la autenticidad de la orden de pago y en segundo lugar si se dispone de saldo suficiente para realizar dicha transacción. En caso que así sea, la orden será atendida. El problema que surge en este caso es del doble gasto, que se corrige suponiendo y creyendo que el banco lleva una contabilidad adecuada y realiza correctamente las tareas de verificación y registro.

Cuando estas transacciones se realizan entre dos bancos diferentes el procedimiento cambia un poco pues no es simplemente restar una cantidad de la cuenta de una persona en el banco A y adicionar ese importe en la cuenta que tiene otra persona en el banco B, sino que ahora es necesario también un ajuste contable entre los dos bancos implicados ya que es necesario o bien que uno de los bancos tenga una cuenta propia en otro banco, o bien la existencia de una tercera entidad financiera o algún sistema de compensación y liquidación interbancaria en el cual tengan a su vez cuenta los dos bancos A y B.

El proceso sería el siguiente: el dinero que sale del banco A tiene que darse de baja tanto en la cuenta de dicho cliente como en la cuenta que el banco tiene a su propio nombre en el tercer banco C o en el sistema de compensación, y debe abonarse en la correspondiente cuenta propia del banco B para que finalmente se pueda realizar el correspondiente abono en la cuenta de la persona a la que va dirigida la transacción tiene en el banco B. [34]

El tercer banco debe de comprobar la autenticidad de la orden que recibe del primer banco y que existe el saldo suficiente para atenderla. Si estamos ante pagos internaciones la cadena se amplía aún más con los correspondientes gastos financieros que acarrean, es decir, a más eslabones en la cadena, mayores comisiones bancarias.

[34] González Meneses, M, 2017: página 35

Según un informe de 2015 de la consultora financiera Oliver Wyman, el coste que supone el sistema de transferencias y compensaciones y liquidaciones se encuentra entre los 65.000 y los 80.000 millones de dólares al año.

Lo que proponen las criptomonedas, el bitcoin en primer lugar, es un sistema de pagos sin la intervención de ninguna entidad financiera y, por lo tanto, prescindiendo del dinero que crean y ponen en circulación los Estados a través de sus bancos centrales. Las criptomonedas persiguen un sistema monetario independiente y autosuficiente, completo y paralelo al tradicional.

La blockchain supone una verdadera revolución porque puede llegar a conseguir la supresión de muchos costes relacionados con la intervención de cualquier agente que preste servicios como por ejemplo de documentación, autenticación o registro, y también de las comisiones propias de la mediación bancaria y por lo tanto lograr un profundo ahorro económico. La blockchain no es una empresa ni una institución ni una organización. Es una aplicación, un programa, una determinada forma de hacer algo. No pertenece a nadie, el libro mayor o registro en que consiste no está a cargo de ninguna empresa ni de ningún particular, sino que es algo que se va formando entre muchos usuarios. Es muy seguro frente a manipulaciones, pero no en cuanto a la forma de acceso a cada registro.

Para las entidades financieras supone una grave amenaza y es por este motivo que algunas de ellas han decido apostar por crear su propia criptomeda, a fin de entrar de lleno en este nuevo mercado.

La banca siempre ha desempeñado la función de custodia de nuestro dinero, es decir, depositamos nuestro dinero en ellos para evitar que se pierda o que nos lo roben. Creemos que en sus manos estará mejor que en las nuestras, incluso si ellos llegan a perder el dinero que tienen depositado en sus oficinas es su problema, pues existe un sistema de garantías que protege a los usuarios de la banca. Al abrir una cuenta de depósito, el dinero se convierte en un crédito contra el banco depositario, así que el riesgo de pérdida se traspasa al banco.

Por el contrario, el bitcoin implica un dinero seguro no susceptible de pérdida ni de sustracción mientras se conserve la clave de seguridad privada y por tanto el usuario del mismo no necesita contar con ninguna entidad financiera. La idea que llevó a cabo Nakamoto era eliminar la figura del intermediario mediante un sistema descentralizado de intercambio de datos, se trata de un sistema de usuario a usuario de dinero electrónico.

¿Puede suponer esto el inicio del fin del sistema bancario? El negocio bancario que hasta ahora conocemos se basa principalmente en los depósitos de dinero que realizan los ahorradores y que los bancos utilizan a su vez para realizar operaciones activas de préstamo. Si con las criptomonedas no vemos necesario guardar el dinero en los bancos puede desaparecer la base de toda la actividad bancaria.

El sector bancario se encuentra en una gran transformación, intentando adaptarse y encontrar su hueco en este nuevo rumbo que toma Internet. Es un nuevo cambio cultural por los cambios de hábitos y consumo a los que estamos asistiendo.[35] En el intento de los bancos de no quedarse fuera, de adaptarse al nuevo entorno algunos de ellos ya han creado su propia criptomoneda como por ejemplo el Banco Santander que se ha alcanzado una alianza con otras 14 entidades financieras internacionales y juntas han creado la Utility Settlement Coin (USC) y través de ella “Fnality”. Se trata de un proyecto en el que gracias a la blockchain los bancos partícipes podrán realizar transferencias de forma instantánea.

[35] Preukschat, A. 2017; páginas 33-34

9.2 ASEGURADORAS

Los seguros también podrían beneficiarse de esta nueva tecnología. Se trata de un sector en completa modernización que ya cuenta con startups digitales y especializadas que utilizan el Big Data para elaborar seguros adaptados a las necesidades de cada persona. La blockchain puede jugar un papel fundamental en este negocio y lograr un aumento del beneficio del sector. Se crearán nuevos modelos de seguros en los que lo más importante será la personificación del mismo, es decir, un seguro hecho a medida a las características del contratante.

Cinco asegurados se han unido para investigar las nuevas posibilidades que puede ofrecer esta tecnología. Han sido Allianz, Aegon, Munich Re, Zurich y Swiss Re. Estas empresas han elaborado una plataforma común denominada "Blockchain Insurance Industry Initiative-B3i" para juntar nuevas ideas, casos de uso y experiencias.[36]

La fortaleza de este tipo de industrias estará en la utilización de los "Smart Contracts" o bien los contratos inteligentes que anteriormente citamos. La gran ventaja que supone es que puede permitir a las aseguradoras actuar en cuanto el riesgo que protegen suceda. Por ejemplo, supongamos el caso de un pasajero que ha comprado un billete de avión con seguro de cancelación y finalmente sucede que el vuelo se cancela. En cuanto esto ocurre la aseguradora le devolverá el importe del vuelo sin tener que hacer ningún trámite ni reclamación. Es decir, la devolución se produce sin que el sujeto tenga que realizar acción alguna porque se trata de un contrato inteligente. En estos casos el cliente queda muy satisfecho con el servicio prestado.

En el caso de las aseguradoras de la rama de la salud, se podría contar con un sistema que relacionase automáticamente los registros médicos. Es decir, si una persona, por ejemplo, llega a un centro médico de otro país, con solo decir su nombre estos puedan acceder a todo su historial. Es un sistema que facilitará todas las comunicaciones, las funciones administrativas y el trabajo de médicos y enfermeros para dotar al cliente de una mayor satisfacción.

Si pensamos en seguros de automóvil, lo más fácil sería que alguien que quiera asegurar su coche enviase a todas las aseguradoras su historial de siniestros de forma anónima. Una vez que recibiese las ofertas de estas, las valoraría y comunicaría la opción elegida. Cuando se identifique y pague la póliza, el seguro ya estaría listo y empezaría a surtir efecto. En caso de accidente o daño, cuando se den las condiciones estipuladas en la póliza para la indemnización, ésta se producirá de forma automática.

Si se trata de un coche inteligente podría indicar a la aseguradora los hábitos de conducción de la persona como los kilómetros que hace a la semana o la velocidad a la que circula. Esto supone una verdadera revolución para este sector al poder saber en todo momento como está el bien asegurado. Los trámites se reducirían y tendría lugar un gran ahorro.

Otro aspecto a destacar es la relación entre los seguros y Big Data. Gracias a esta última, las aseguradoras pueden conocer mejor a sus clientes y por lo tanto ofrecerles un mejor servicio. Por ejemplo, si la aseguradora sabe que tiene un buen cliente gracias a los datos de los que dispone le ofrecerá una buena oferta y a largo plazo obtendrá su fidelidad. Por el contrario, también sirve para detectar aquellos que hacen mal uso de los servicios y evitar grandes pérdidas. Además, cabe resaltar que, gracias a disponer de más datos sobre los

[36] Preukschat, A. 2017, página 44

clientes, las aseguradoras podrán predecir los riesgos a los que se enfrentan y personalizar los productos.[37]

9.3. OTRAS POSIBLES APLICACIONES

Otra aplicación posible la vemos en el campo de la contabilidad y auditoría. La labor de los auditores es necesaria para verificar las cuentas de las empresas y a la vez es un proceso muy largo y costoso. Aplicando esta nueva tecnología, todas las operaciones pueden quedar en una base de datos única y compartida desde el momento en el que se realicen y que, por lo tanto, puedan ser verificadas a la vez. Es decir, se podrá verificar la información de forma inmediata ahorrando procesos y costes.

La Agencia Tributaria sería una de las grandes beneficiadas en su aplicación. Si tanto la agencia como la empresa comparten una misma blockchain se podría ir elaborando sobre la marcha los impuestos que debe presentar la empresa de forma automática, lo que permite un gran ahorro de tiempo y costes a la vez que supondría una transparencia total y ausencia de fraude, algo muy difícil de conseguir hoy en día. Se podría saber en cualquier momento el estado de la contabilidad de cada empresa y acabar con el fraude y blanqueo de capitales.

Las ONG también están empezando a usar este sistema. Hasta ahora, el donante no quería que una parte importante de su donación se quedase en manos del intermediario, y además domiciliar pagos de uno o dos euros al mes o hacer estas transferencias periódicas no les salía nada rentable. Con la blockchain se pueden realizan estas donaciones en cualquier momento y sin que ningún intermediario se quede con ninguna parte de la aportación. La financiación de las ONG puede ser tanto pública como privada y con esta tecnología se puede seguir el todo momento el rumbo que toma dicha financiación, es decir, a que se destina y en qué momento y lugar. Supone una total transparencia que aumenta la confianza de los donantes a la vez que acaba con la corrupción y la mala gestión. [38]

10. NUEVAS FORMAS DE FINANCIACIÓN EMPRESARIAL: LAS ICO

Las ICO “Initial Coin Offering” suponen una nueva forma de financiación empresarial basada en la Blockchain. Según la ESMA (Autoridad Europea de Valores y Mercados), las ICO son una nueva vía para captar fondos del público por parte de las empresas a través de criptomonedas o tokens. Es decir, su objetivo fundamental es la financiación de proyectos en su mayoría relacionados con el Internet del valor.

Un token es la pieza central en torno a la cual gira este nuevo modelo económico. Podemos definirlo como ficha, pieza o prueba, y representan el valor de algo. Las criptomonedas con la primera y más conocida representación de los tokens, pero no la única.

El método de las ICO es el siguiente: comienza con un documento que describe el proyecto y los derechos que se otorgan a los inversores. Normalmente, este documento determina la cantidad máxima y mínima de monedas que se deben suscribir para que el proyecto tenga futuro. La empresa pone en venta monedas o tokens, normalmente bitcoins o Ether, a cambio de divisas tradicionales u otras criptomonedas con la finalidad de recaudar fondos.[39]

[37] https://www.inese.es/big-data-y-seguros-la-revolucion-que-ya-esta-en-marcha/

[38] Preukschat, A. 2017

[39] BARSAN I. M., (2017) LL.M. Legal Challenges of Initial Coin Offerings (ICO). Revue Trimestrielle de Droit Financier (RTDF), n° 3, pp. 54-65

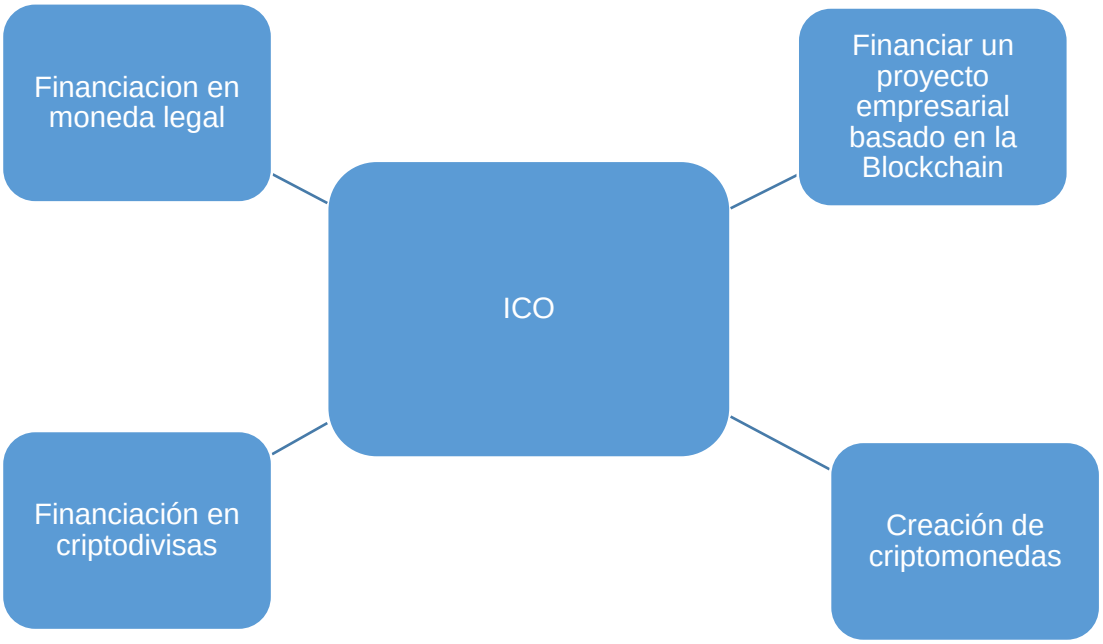
Es una forma de financiación a la que recurre sobretodo pequeñas empresas y start-ups cuando comienzan su aventura empresarial. Se usan en su mayoría para dos tipos de proyectos: la creación de una nueva criptomoneda o la financiación de una aplicación del Blockchain. No depende de ninguna institución y son las propias personas las que ofrecen su dinero y como contrapartida pueden:

1. Comprar un producto o servicio que el ofertante desarrolla utilizando la blockchain
2. Otorgar derechos de participación en los activos futuros de la empresa
3. La negociación futura de los tokens en los mercados en forma de criptomonedas.

Para sacar el máximo partido posible a esta nueva forma de financiación, los inversores deberán invertir tras haber estudiado y conocido los posibles riesgos de este tipo de operaciones, a saber:

1. Marco regulatorio de la operación: en España se considera que las operaciones con ICOs deberían ser tratadas como emisiones u ofertas públicas de valores negociables.
2. Modelo de negocio: si el modelo de negocio que sustenta una ICO no funciona, la inversión presenta todas las cartas para no tener éxito, al igual que en cualquier inversión tradicional. [40]

Gráfico 8: Principales funciones de las ICO



FUENTE: Elaboración propia

La ICO que más triunfó en los últimos años ha sido el proyecto del Ethereum, que recaudó cerca de quince millones de euros. Los inversores han multiplicado hoy el día por 50 su inversión inicial.

Como inconvenientes destacaremos que la moneda puede fracasar o que la pueden robar. Según Ernest & Young, cerca del 10% del capital de las ICO se pierde por ataques informáticos y hackeos.

[40] Guaita Martínez, J.M. (2019): Las criptomonedas: Digitalización del dinero 2.0. Pag 120-122

Por otra parte, las ICO también presentan varios riesgos que enumeraremos a continuación:

1. Falta de regulación y vulneración frente al fraude. Las inversiones no suelen estar protegidas ni amparadas por el derecho de la Unión Europea.
2. Alto riesgo de perder todo el capital invertido ya que las empresas que las emiten suelen estar en su fase inicial y por lo tanto puede fracasar y no ofrecer el rendimiento esperado.
3. Es posible que el capital no sea reembolsado. Aunque el proyecto salga adelante, quizás la criptomoneda no saliese el mercado y por lo tanto no fuese posible intercambiar la criptomoneda por moneda de curso legal.
4. Se pueden dar asimetrías en la información entre empresa e inversor.

Según la Comisión Nacional del Mercado de Valores, CNMV, toda ICO debe cumplir una serie de requisitos:

1. La directiva sobre folletos
2. La directiva sobre mercados e instrumentos financieros
3. Directiva sobre gestores de fondos de inversión y alternativa
4. Directiva antiblanqueo de capitales.

En definitiva, las ICO son una nueva forma de financiación que probablemente tenga gran éxito en el futuro gracias a un mecanismo sumamente práctico por su carácter flexible y descentralizado y por su escasa regulación. Además, como las campañas de ICOs se desarrollan principalmente por internet es importante tener abiertos canales de comunicación flexibles, ágiles y controlados ya que se han dado casos de estafadores que crearon links similares al del proyecto para conseguir beneficios de manera ilegal.

11. CONCLUSIONES

A lo largo del presente trabajo hemos visto como estamos asistiendo a un nuevo sistema que puede revolucionar la sociedad tal y como la conocemos hoy en día gracias a su capacidad de registrar todo tipo de transacciones persona a persona de manera eficiente, segura, verificable e inmutable, lo que significa que puede aplicarse a tareas no financieras como la contabilidad o la trazabilidad de productos en la cadena de suministro, se trata de un fenómeno social sin precedentes ya que nos hace replantearnos seriamente el concepto del dinero. Surgió como consecuencia de buscar una respuesta a las carencias del actual sistema financiero que salieron a la luz con la crisis del 2008. Lo que se pretende es un gran cambio de conciencia en el que la confianza que antes se depositaba en las instituciones oficinales y privadas ahora recaiga sobre un sistema descentralizado basado la tecnología blockchain. No cabe duda de que se trata de un gran avance para la sociedad pero como todo avance lleva su tiempo y aunque la mayoría de criptomonedas han tenido una rápida aceptación en el sistema económico y financiero, sus propias características como ser emitidas sin el respaldo de un banco central, la alta volatilidad de sus cotizaciones, y el desconocimiento de la mayoría han reducido su uso como medio de pago además de que pueden surgir dudas en cuanto al cumplimiento de las otras dos funciones: unidad de cuenta y depósito de valor.

Por otro lado, la regulación es muy difusa y compleja al carecer de uniformidad a nivel mundial. Se trata de materias permitidas pero que no están reguladas específicamente. Al tratase de un modelo relativamente nuevo tiene sus debilidades y es que su aceptación como medio de pago no se ha producido de forma generalizada, su carácter anónimo fomenta su uso en actividades ilícitas y su seguridad a veces se ha puesto en duda como consecuencia de robos a exchanges, fraudes, etc.

Cabe destacar sobre todo que las criptomonedas son una de las muchas aplicaciones de la tecnología blockchain pero ni la única ni seguramente sea las más relevantes por lo que el futuro de esta tecnología no está comprometido por el de las critomonedas. Una de las opciones que seguramente veamos en el futuro sea un escenario en el que las criptomonedas coexistan como nuevas formas de dinero con el dinero fiduciario.

Para que podamos hablar de un sistema instaurado tiene muchos puntos que mejorar como consolidarse como medio de pago y además falta mucho camino en su regulación, debe conseguirse una legislación abierta y uniforme. Además, una de las mayores amenazas que presenta es el posible aumento de actividades de blanqueo de capitales, por lo que los gobiernos deben regularizar específicamente su uso y posibles aplicaciones con el fín de erradicar estos posibles fraudes. También se debe perseguir un mercado eficiente ya que si no faltará interés en los intermediarios financieros. La confianza entre los participantes depende de la confianza en la tecnología pero ésta no está completamente libre de vulnerabilidades, incluidos los errores accidentales y los ataques maliciosos en las aplicaciones que se asientan sobre la cadena de bloques. Además, la automatización tampoco eliminará los conflictos de interés o la corrupción. A pesar de que los defensores de la blockchain promulgan su inviolabilidad nadie está exento de fallos.

Por otro lado, si bien blockchain promete un mundo en el que los intermediarios que conocemos no son necesarios, aún pueden ser posibles. Por ejemplo, a partir de internet las agencias de viajes no eran necesarias pues cualquier puede reservar vuelos, hoteles y viajes completos sin necesidad de ellas pero esto no implica que desaparezcan. El hecho de que podamos hacer un contrato directamente no implica que tengamos los conocimientos o el tiempo necesario para llevarlo a cabo, así que estos costes incentivan el uso de intermediarios a pesar de no necesitarlos.

BIBLIOGRAFIA

LEGISLACIÓN:

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

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

REFERENCIAS BIBLIOGRAFICAS:

Domingo, C. (2018): *"Todo lo que querías saber sobre Bitcoin, Criptomonedas y Blockchain y no te atrevías a preguntar".* Editorial Planeta.

Guaita Martínez, J.M. (2019): *Las criptomonedas: Digitalización del dinero 2.0.* Editorial Aranzadi.

González Meneses, M (2017): *"Entender Blockchain".* Editorial Aranzadi.

Preukschat, A. (2017): *"Blockchain: La revolución industrial de Internet"* .Editorial Planeta.

Boar, A. (2018): *"Descubriendo el blockchain".* Editorial Profit.

Navas Navarro, S. (2015): *"Un mercado financiero floreciente: el del dinero virtual no regulado (especial atención a los BITCOINS)",* en Revista CESCO de Derecho de Consumo.

Vicente, N. (11 de abril de 2020): *El coronavirus amenaza con poner fin al dinero en efectivo antes de lo previsto.* El economista.

Barsan, I.M. (2017): *Legal Challenges of Initial Coin Offerings (ICO).* Revue Trimestrielle de Droit Financier (RTDF), n° 3.

Vivanco, F; Keller, L. (3 de mayo de 2019): *Las ventajas de enviar dinero digital*. El País.

Pacheco Jimenez, Mª N (2016): "*Criptodivisas: del bitcoin al MUFG. El potencial de la tecnología blockchain*" en Revista CESCO de Derecho de Consumo, núm. 19.

PÁGINAS WEB CONSULTADAS:

Mentes Criptomillonarias: https://criptomonedaonecoin.wordpress.com/2017/03/18/el-origen-y-la-evolucion-del-dinero/

Portal Cliente Bancario del Banco de España: https://clientebancario.bde.es/pcb/es/menu-horizontal/productosservici/serviciospago/Dinero_electronico.html

The Nielsen Company: https://www.nielsen.com/do/es/insights/report/2017/estudio-global-comercio-conectado/

Etoro: https://www.etoro.com/

El Mundo digital: https://www.elmundo.es/elmundo/2013/02/14/navegante/1360826212.html

Blockgeeks: https://blockgeeks.com/guides/es/que-es-ethereum

CoinMarketCap: https://coinmarketcap.com/es/

Bitcoin projet 2009-2020: https://bitcoin.org/bitcoin.pdf

El Economista: https://www.eleconomista.es/diccionario-de-economia/dinero-electronio

El País digital: https://elpais.com/elpais/2019/05/02/planeta_futuro/1556802491_797658.html

Blog criptomonedaonecoin: https://criptomonedaonecoin.wordpress.com/2017/03/18/el-origen-y-la-evolucion-del-dinero/

Oro información: https://oroinformacion.com/que-es-y-como-funciona-el-patron-oro/

IG: 2003-2020 https://www.ig.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas

CYSAE: https://cysae.com/

UniMOOC: https://blog.unimooc.com/bitcoin-definicion-caracteristicas/

BLOCKGEEKS: https://blockgeeks.com/guides/es/que-es-ethereum