Universidad Zaragoza
1542

Trabajo Fin de Grado

"Las criptomonedas, el blockchain y su comparativa con las divisas"

"Cryptocurrencies, the blockchain and its comparison with currencies"

Autor/es

Sergio Giménez Gil

Director/es

Aurora Sevillano Rubio

Facultad de Economía y Empresa de la Universidad de Zaragoza

2021

ÍNDICE

1. INTRODUCCIÓN

1.1. OBJETIVOS

Con motivo de la creciente repercusión del fenómeno de las criptomonedas tanto en la economía como en la sociedad actual, pretendo con este trabajo dar una visión general del funcionamiento de las criptomonedas, en concreto, del bitcoin. El objetivo principal es obtener la mayor cantidad de información posible acerca de esta tecnología de reciente creación para entender su funcionamiento, la importancia que puede tener en el ámbito de las inversiones y las principales diferencias de este tipo de monedas con las divisas tradicionales. Además, pretendo exponer la consideración del bitcoin como divisa o como commodity [1] según lo expuesto por los diferentes organismos internacionales. Otro objetivo a destacar sería la determinación de la rentabilidad en la inversión en criptomonedas, concretamente la inversión en bitcoin.

Con todo lo expuesto anteriormente pretendo colegir en qué mercado interesaría invertir de forma más favorable para un potencial inversor, en el mercado de las criptomonedas o en el mercado de las divisas, teniendo en cuenta los riesgos y la evolución de los precios en ambos mercados. Para determinar la inversión en el mercado de las divisas me centraré en las dos principales divisas existentes (Euro y Dólar) mientras que en el caso de las criptomonedas me centraré en la criptodivisa más importante, el bitcoin.

1.2. MOTIVACIÓN

Motivado con la creciente importancia de las criptomonedas en la actualidad y durante los meses de cuarentena que tuvimos que vivir, empecé a investigar acerca del mundo de las criptomonedas. Tras pasar muchas horas leyendo numerosos artículos vía online y visualizar videos de YouTube donde se explicaba todo el funcionamiento de las criptomonedas, decidí invertir. Una inversión mínima, donde quería aprender y vivir personalmente la volatilidad de las "monedas virtuales". Me puse en contacto con dos amigos míos de forma que decidimos observar, en nuestro tiempo libre, la evolución de los precios de las criptomonedas a través de la página web www.tradingview.com, en

[1] Una commodity es un bien físico o mercancía que se consume directamente, es decir, que no es sometido a ningún proceso de transformación de forma que es comercializado en su estado original. Un ejemplo claro de commodity es el oro.

concreto Chainlink, que fue la moneda en la que decidimos invertir. Observábamos los gráficos determinando el precio máximo y mínimo a que podría llegar la moneda en esa semana concreta, de forma que tras un mes de estudio decidimos vender obteniendo una rentabilidad del 200% con respecto a nuestra inversión inicial.

Por ello, y tras una primera reunión con Aurora Sevillano Rubio, la cual me propuso el tema de las criptomonedas, decidí realizar el TFG acerca de esta área con el objeto de incrementar mis conocimientos en el citado ámbito.

1.3. METODOLOGÍA

En primer lugar, haré referencia al origen de las criptomonedas, sus características generales y la financiación a través de las criptomonedas. Determinaré la regulación legal existente en la actualidad en el ámbito de las criptodivisas y realizaré una reflexión sobre la naturaleza de las monedas virtuales como dinero o como commodity, indicando también la clasificación realizada por los organismos internacionales.

Seguidamente, me centraré en el Blockchain como una especie de libro contable donde se registran cada una de las transacciones con criptomonedas que se registran. A continuación, centraré la atención en el Bitcoin como principal "moneda virtual" y otras criptomonedas o "altcoins".

Por último, y debido a la importancia que tiene según mi punto de vista, realizaré una comparativa entra las divisas y las criptomonedas, exponiendo la evolución de los precios desde el año 2008 hasta la actualidad. Realizaré la comparativa desde el año 2008 porque es el año en el que aparece el bitcoin, por lo que considero que puede ser interesante estudiar la evolución del precio del bitcoin desde su creación hasta la actualidad, para poder observar también el efecto del fenómeno "halving" en el precio de la citada moneda virtual.

2. LAS CRIPTOMONEDAS

2.1. CONSIDERACIONES GENERALES DE LAS CRIPTOMONEDAS

2.1.1. ORÍGENES

El origen de las criptomonedas[2] o criptodivisas se establece en los años 80, cuando en búsqueda de un medio para obtener cambios sociales y políticos aparece un movimiento denominado Cypherpunk[3]. Este movimiento pretendía escribir claves secretas que no podrían ser descifradas por personas que no tuvieran los conocimientos tecnológicos suficientes para ello.

Ya en la década de los 90, un criptógrafo y matemático estadounidense, bajo el nombre de David Chaum inventó una variante de dinero digital, "Digicash". A través de este medio, David estableció una forma de dinero electrónico centralizado que habilitaba para la realización de transacciones seguras y anónimas. Años más tarde, en 1997, Adam Black, con el objeto de combatir el spam creó "HashCash" basándose en la prueba de trabajo. Para muchos analistas este software permitió determinar los pilares para establecer los protocolos de seguridad y minería que inspirarían las criptomonedas futuras. Un año más tarde, en 1998, Wei Dai diseña b-money. B-money fue una propuesta creada con el objetivo de diseñar un sistema de dinero electrónico que fuera anónimo y que, además, estuviera distribuido. Pese a que b-money no se implementó finalmente, para muchos es considerada como la primera criptomoneda real ya que el sistema que se propuso para la misma es muy similar al sistema teórico[4] de las criptomonedas actuales.

No fue hasta 2009 cuando un desarrollador bajo el pseudónimo Satoshi Nakamoto crea la primera criptomoneda, el Bitcoin.

[2] Las criptomonedas son monedas digitales las cuales no se encuentran en soporte físico pero que, independientemente de ello, sirven para realizar intercambios de bienes y servicios. Se consideran un medio de pago, al igual que las divisas, con la particularidad de que no son controladas ni por Estados ni por Bancos.

[3] Se entiende por Cypherpunk como aquella persona cuyas ideas le llevan a un activismo a favor del uso de la criptografía y la tecnología con el objeto de proteger el ámbito privado de las personas.

[4] El sistema teórico es muy parecido al esquema Prueba de Participación que se utiliza en el sistema de criptomonedas actual.

2.1.2. CARACTERÍSTICAS GENERALES DE LAS CRIPTOMONEDAS

En primer lugar, debemos definir qué se entiende por criptomoneda. La criptomoneda o criptodivisa es un tipo de moneda basado en el sistema criptográfico[5] cuyo fin esencial es proporcionar una modalidad de pago segura. Mediante el sistema criptográfico referido se regula la producción de unidades monetarias y se verifica la realización de transferencia segura de fondos. Es decir, las criptomonedas son monedas virtuales que actúan como un medio de pago intangible y descentralizado alternativo al dinero tradicional, pudiendo realizar operaciones mediante un cifrado digital (que le otorga seguridad), sin que sea necesaria la existencia de intermediarios (como son los bancos). Actualmente, existen plataformas digitales que se podrían confundir con las criptomonedas, como es el caso de PayPal. Sin embargo, PayPal cuenta con un sistema centralizado, mientras que las criptomonedas se caracterizan por su descentralización. Un aspecto importante y esencial de las mismas es que se trata de una moneda digital, es decir, no existen físicamente. Pese a ello, otorgan la facultad a los tenedores de las mismas de realizar transacciones instantáneas a través de internet.

La Dirección General de Operaciones, Mercados y Sistemas de Pago del Banco de España considera las monedas virtuales (entra las que se encuentra el bitcoin) como *"un conjunto heterogéneo de instrumentos de pago innovadores que, por definición, carecen de un soporte físico que los respalde"*.

Pero las criptomonedas se caracterizan por tener una serie de rasgos comunes que llevan a justificar tanto su operabilidad como su valor económico. Independientemente de las características propias de cada criptomoneda existente, éstas poseen unas características comunes que podemos determinar en las siguientes:

- ***Descentralización:*** Es una característica esencial de las criptomonedas. Con "descentralización" nos referimos al hecho de que este tipo de moneda digital no se encuentra controlado ni regulado por ningún país, gobierno o banco. A razón de ello, el valor de las mismas únicamente quedará determinado por el mercado,

[5] La criptografía consiste en la utilización de códigos y cifrados para otorgar seguridad al usuario. Los códigos son procesos a través de los cuales el remitente modifica cierta información (lo que se denomina cifrado) para hacer dicha información ilegible a todos menos al destinatario, que conoce el código y por tanto puede conocer la información.

sin que ningún banco, país o gobierno pueda interferir en el referido valor. Además, las criptomonedas sólo se trabajan por medio de internet, otro aspecto clave para evitar ese control al que nos hemos referido.

- ***Operatividad:*** El hecho de tratarse de un tipo de moneda que no se encuentra regulado por ningún mercado oficial supone que se pueda operar con las mismas las 24 horas del día durante los 365 días del año. Esta operatividad de las criptomonedas es un aspecto muy interesante para el uso de las mismas por parte de las empresas ya que, para realizar una transacción únicamente se precisa de un oferente y un demandante. Como consecuencia de ello, las empresas evitan el pago de comisiones a terceros.
- ***Confidencialidad:*** Las criptomonedas ostentan un código computarizado que únicamente puede ser conocido por aquellas partes que realizan el intercambio. Ello conlleva que para realizar una transacción no sea necesario proporcionar los datos personales de las partes. Supone una gran ventaja, pero al mismo tiempo un gran inconveniente, pues la utilización de este medio de pago puede ser utilizado para la comisión de actividades ilícitas.
- ***Transparencia:*** Todas y cada una de las transacciones que se realizan en el mercado virtual de las monedas digitales son registradas en un "libro contable" el cual está compartido en la red del blockchain y es imposible o muy difícil de manipular.
- ***Volatilidad:*** Es otra de las características esenciales de las criptomonedas. Como ya hemos indicado, se trata de monedas digitales descentralizada, de forma que pueden sufrir variaciones importantes en su valor. Esta característica favorece especialmente el "trading" [6] con criptomonedas, es decir, la negociación o especulación con estas.
- ***Aceptación:*** El valor de las criptomonedas viene determinado por la valoración que hagan los individuos de estas. Es decir, vendrá determinado por el valor que estos individuos estén dispuestos a pagar por ellas, y otros para vender.
- ***Limitadas:*** No existe un número ilimitado de criptomonedas debido a su forma de producción. A diferencia de las divisas tradicionales donde se imprimen billetes y monedas, la producción de criptodivisas es muy diferente ya que se

[6] Se entiende por "trading" de criptomonedas como el hecho de especular en base a los movimientos de los precios de las criptodivisas a través de una cuenta de "trading" de CFD (derivado financiero similar a los futuros y opciones) o la compra y venta de criptomonedas.

crean a través de la minería [7]. Algunas de las monedas existentes son deflacionarias [8] como el Bitcoin (se prevé que la cantidad de Bitcoins en circulación no exceda de 21 millones).

- ***Inmediatez:*** Las operaciones con criptodivisas ostentan una gran celeridad en la realización. Ello es un aspecto muy importante ya que, por ejemplo, en el caso de empresas que tengan clientes internacionales (de países con los que no exista un tratado) podrán realizar transacciones instantáneas con ellos a través de este medio, sin tener que esperar varios días a que la operación culmine con éxito.
- ***Desregularización:*** Actualmente las criptomonedas no están reguladas por ninguna ley. Ahora bien, en septiembre de 2020, varios países de la UE entre ellos España han propuesto la creación de un organismo específico para la regulación de las criptomonedas.
- ***Accesibilidad:*** Es una de las características esenciales de las criptomonedas. Cualquier persona puede adquirir criptomonedas, crearse una wallet[9] y comenzar a recibir y enviar monedas. Podemos diferenciar dos formas de obtener una criptomoneda. La primera forma consistiría en ser minero, es decir, crear nuevas unidades de una determinada criptomoneda. Ahora bien, minar una moneda es un proceso complejo que precisa de criptografía avanzada y sistemas de comprobación que suponen cálculos matemáticos excesivamente complejos. Ello, unido con la gran cantidad de energía computacional necesaria para generar una unidad de criptomoneda hace que sea una opción de difícil acceso para una persona que no cuente con los medios o conocimientos citados. La otra forma, y mucho más sencilla y accesible consiste en comprar criptomonedas a empresas o personas que las tengan. Esta última opción se podría llevar a cabo a través de las

[7] La minería consiste en resolver un problema matemático mediante equipos informáticos por parte de los mineros (o personas que utilizan sus ordenadores o equipos especializados en la resolución de estos problemas matemáticos). Cuando se resuelve el problema matemático, se obtendrán como recompensa una determinada cantidad de criptomoneda, que posteriormente el minero venderá para obtener recursos para pagar por ejemplo la cantidad de energía que haya utilizado en resolver el problema matemático. Por ejemplo, en el caso del oro es necesario tener maquinaria específica para su extracción. De ahí viene el concepto de minería en las criptomonedas, es decir, tener un equipo informático específico para poder resolver los problemas matemáticos que se proponen a los mineros.

[8] Por monedas deflacionarias entendemos aquellas monedas que ganan valor con el paso del tiempo ya que habrá menos cantidad de monedas disponibles.

[9] Una wallet o monedero de criptomonedas es una cuenta que permite al usuario almacenar, enviar y recibir criptomonedas.

denominadas casas de cambio[10], las cuales desarrollaré más en profundidad con posterioridad.

Una vez determinadas las características comunes de todas las criptomonedas, debemos indicar las ventajas y desventajas que tienen.

Una de las ventajas que tienen las criptomonedas son sus bajas tasas de transacción, especialmente en transacciones internacionales. Cuando un usuario envía dinero tradicional a otro país pagará una comisión por la transacción. Mediante las criptomonedas esta comisión desaparece de forma que se permite enviar cierta cantidad de criptomonedas de forma prácticamente instantánea a coste nulo. Otra ventaja sería la independencia para el uso de las criptomonedas de bancos. Es decir, las criptomonedas pueden ser usadas en cualquier lugar del mundo (lo único que se necesita es un ordenador o un móvil para poder operar con él) mientras que con el dinero tradicional precisas de una cuenta bancaria en un banco. Pero sin duda, la mayor ventaja que presenta es la reiteradamente referida descentralización. Mediante esta descentralización, no se depende de terceros pues cada transacción que se realiza se produce en la red, quedando almacenada en esa misma red. Así, cualquiera puede comprobar las transacciones que se hayan realizado otorgando al sistema de una gran transparencia. De esta forma, cualquiera puede comprobar cuándo se realizó la transacción, pero manteniendo la privacidad de las personas pues, aunque los números de wallet o cartera son públicos, no aparece recogido a quién pertenece cada cartera. En definitiva, en las criptomonedas no existe restricción alguna, pues puede operar con este tipo de monedas en cualquier momento.

Esta falta de restricciones ha favorecido el uso de las criptomonedas para llevar a cabo transacciones ilegales como pueden ser el tráfico de drogas o la trata de personas. Otra desventaja sería la posible pérdida del dinero ya que, si tienes una cartera de clave privada (la cual se caracteriza por tener una clave para poder acceder a tu cartera) y la pierdes, pierdes todo el dinero que tenías en la misma. Además, las criptomonedas se caracterizan por tener grandes fluctuaciones en el precio que unidas con el desconocimiento que pueden otorgar las monedas virtuales genera desconfianza en los usuarios.

[10] Podríamos definirlas de forma análoga a las oficinas de cambio de divisas, es decir, actúan como intermediarios entre los usuarios.

2.1.3. EL BLOCKCHAIN COMO "JUSTIFICANTE" DE LAS TRANSACCIONES EN CRIPTOMONEDAS

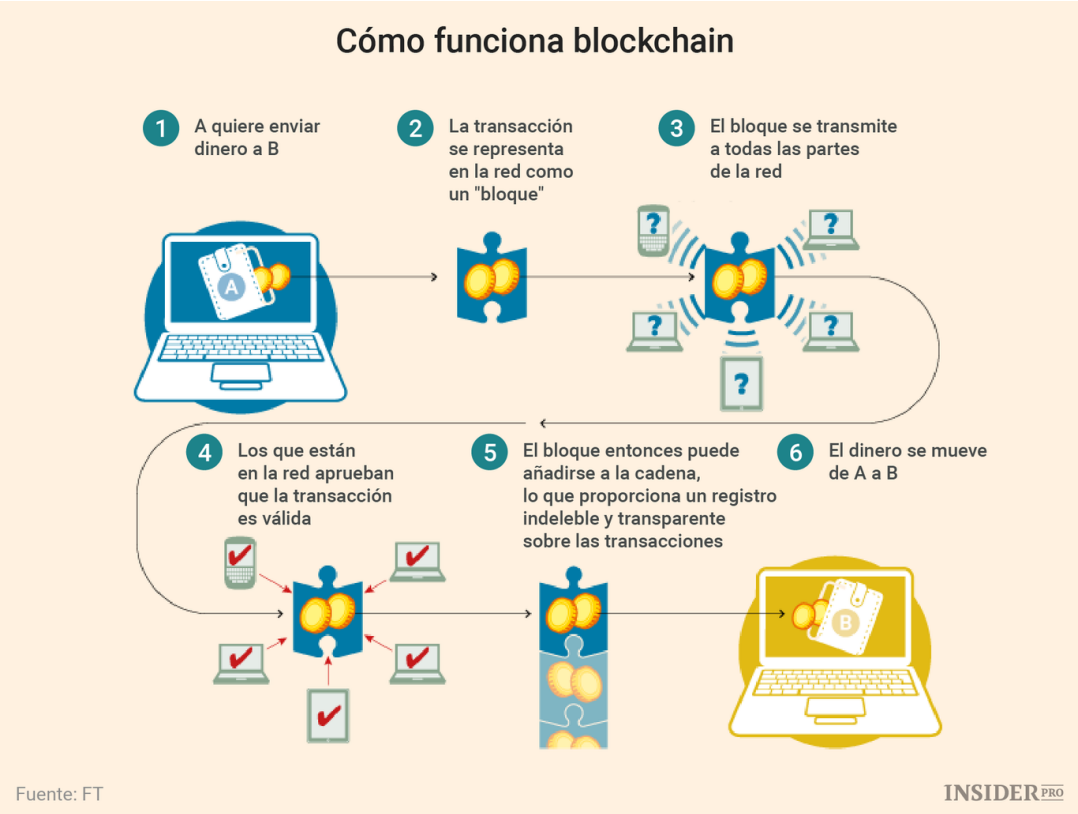
El Blockchain o cadena de bloques surge como consecuencia de la aparición de las criptomonedas, concretamente tras la publicación de Satoshi Nakamoto, en su libro blanco[11] sobre bitcoin. Satoshi Nakamoto considera que la moneda electrónica es una cadena de firmas digitales, a través de la cual el tenedor de una moneda puede transferirla a otra persona incorporando al final de la cadena la firma digital del código de la transacción anterior y la llave pública del nuevo propietario.

Para una mejor comprensión sobre el funcionamiento de la blockchain propongo un ejemplo aclarativo. Imaginemos que queremos enviar 100 euros a otra persona. Tradicionalmente, iríamos al banco y ordenaríamos que se realizara una transacción por ese importe a otra persona. Nuestro banco, comprobaría que efectivamente tenemos esos 100 euros en la cuenta corriente y ordenaría al banco de la otra persona el deber de ingresar en la cuenta de la otra persona los 100 euros. A cambio, nuestro banco nos cobraría (normalmente) una comisión por la transferencia y los 100 euros llegarían a su destinatario en un plazo de alrededor de dos días. Con la red blockchain este banco desaparece. Nosotros ordenamos que se traspasen 100 bitcoins a otra persona de forma que todos los nodos de la red comprobarán que tenemos esa cantidad de criptomonedas y que no las hemos transmitido anteriormente. Una vez que comprueban este aspecto, la transacción es validada y registrada en la red, de forma que la otra persona recibirá esos 100 bitcoins de forma inmediata y a coste nulo. Es decir, aquí ya no se depende de un único intermediario, sino que son los nodos de la red los que registran y autorizan la operación. Además, en los sistemas tradicionales tanto el transmitente como el beneficiario de la transacción son conocidos, es decir, se conoce su nombre mientras que en el caso de la red blockchain se caracteriza por la imperatividad del anonimato.

[11] El libro blanco es un documento de una extensión moderada (consta de 9 páginas) cuya finalidad esencial era asentar las bases o aspectos esenciales sobre el sistema del Bitcoin y los principios que iban a regir su funcionamiento. Los aspectos más importantes que establece son: necesidad de una red usuario a usuario, define el concepto de moneda digital, implementa la prueba de trabajo (Proof of work), define incentivos para animar a la creación de criptomonedas, necesidad de espacio en el disco duro, verificación de pagos, privacidad e inexistencia de la palabra blockchain (no se nombra con tal en ningún momento. En definitiva, una especie de guía inicial sobre el Bitcoin, su creación, funcionamiento y ventajas que supondría su implantación.

El principal objetivo de este sistema es determinar que el tenedor de la moneda tiene la propiedad de la misma y que no se está produciendo una duplicidad de transacciones. Para conseguir este objetivo se deben conocer todas las transacciones anteriores. Así, Blockchain ofrece a los participantes del sistema el acceso público a las transacciones realizadas de forma que son ellos mismos los que determinan que solo existe una "verdad" registral. Esta verdad está codificada en una cadena en forma de bloques que se encuentra distribuida en todos los nodos o participantes de la red, lo que lo diferencia del sistema de intermediarios tradicional donde la información se encuentra almacenada en un único servidor (el banco en cuestión). De esta forma, cualquier participante de la red tiene facultad para solicitar que se registre una transacción en la cadena de bloques, pero esta transacción debe ser aceptada por todos los usuarios de la red, es decir, todos los participantes de la red van a comprobar que la transacción que se pretende registrar es legítima. Esta comprobación por parte de todos los usuarios es lo que se conoce como minería o *mining*. En este sentido, cada uno de los participantes comprobará que el potencial transmitente de la moneda es el propietario de la misma y que ésta no ha sido traspasada con anterioridad.

Imagen 1. Funcionamiento Blockchain



Fuente: Xakata

Una vez que la transacción ha sido registrada en la red por todos los usuarios, ésta pasa a formar un nuevo bloque en la cadena. Las posibilidades de eliminar este nuevo bloque son prácticamente nulas. Ello es debido al hecho de que todos los participantes de la red tienen la información de la transacción, de forma que, si alguien intentara "hackear" este registro, tendría que atentar a todos los usuarios del sistema. Por tanto, no puede haber una red de registro falsa puesto que todos los usuarios de la red tienen una copia original de la transacción. En el *Anexo 1* se presentan las distintas modalidades de blockchain existentes.

2.1.4. LA MINERÍA COMO FORMA DE ENCRIPTAR LAS TRANSACCIONES EN CRIPTOMONEDAS

La minería de criptomonedas consiste en la resolución de un problema matemático mediante equipos informáticos dentro de una blockchain o cadena de bloques. Cuando alguno de estos equipos informáticos resuelve el problema matemático, se obtendrá una cierta cantidad de la criptomoneda que se esté minando, poniendo en circulación la cantidad de criptodivisa que se haya obtenido. Es decir, una vez que los mineros hayan obtenido esa cantidad de criptomoneda, la pondrán a la venta para hacer frente a los gastos de energía que hayan incurrido en la resolución del algoritmo matemático.

La minería tiene dos métodos principales: PoW (Poof of Work) o PoS (Proof of Stake). Este tipo de algoritmos permiten la distribución de la totalidad de las criptomonedas minadas.

El algoritmo PoW (Poof of Work o "Prueba de Trabajo") está diseñado con el objetivo de otorgar seguridad al sistema, de forma que no se produzcan acciones maliciosas en la red. Su funcionamiento es sencillo, pudiendo dividir el mismo en cuatro etapas. La primera de ellas consiste en el hecho de que un nodo[12] establezca una conexión con la red. Una vez establecida esta conexión con la red, ésta le requiere la realización de una tarea costosa de forma que, si la resuelve, el nodo recibirá una recompensa económica. Una segunda etapa consistente en la resolución de la tarea propuesta. En esta etapa el nivel de consumo de potencia del ordenador es enorme. Esta segunda etapa es lo que se

[12] Los nodos están constituidos por una serie de ordenadores conectados entre sí y simultáneamente a la red de una criptomoneda, ejecutando el software que permite su funcionamiento.

conoce como minería (es decir, la resolución de un problema matemático mediante equipos informáticos). La tercera etapa consiste en la presentación de la solución de la tarea propuesta a la red con el objeto de que se produzca la verificación del cumplimiento de los requisitos exigidos. En caso de que los cumpla se autoriza el acceso a los recursos de la red, pero en caso de que no se cumplan los requisitos se rechazará el acceso a los recursos de la red y por ende la solución propuesta a la tarea propuesta. La cuarta etapa, consiste simplemente en el acceso por parte del nodo o cliente a los recursos de la red y la recepción de la recompensa económica citada en la primera etapa.

El algoritmo Proof of Stake o "Prueba de Participación" tiene un funcionamiento totalmente distinto al de "Prueba de Trabajo". Este protocolo busca que los participantes en la red tengan continuamente el mayor número de monedas posible. Así, cuanto mayor sea la cantidad de monedas que tienen los participantes en la red, mayor será la posibilidad de ser seleccionados para realizar tareas que les van a proporcionar ganancias económicas. Es decir, lo que se busca con este algoritmo es que los participantes en la red validen las transacciones que se dan en la red o crear nuevos bloques. La asignación de estas tareas no se realiza de forma que es el nodo el que se conecta a la red y elige la tarea a realizar, sino que es la red la que selecciona de forma aleatoria a un nodo para que valide un determinado bloque, recibiendo el nombre de validador. Esa selección aleatoria, como he señalado se hace de forma aleatoria, pero redunda en la obviedad que contra mayor sea el número de monedas que tenga un nodo mayor será la probabilidad de ser elegido (tienen más reservas y mayor peso en la red). El objetivo principal de este algoritmo, igual que he indicado con el algoritmo Poof of Work esta establecer un consenso entre todas las partes que forman la red. Para dar una visión más clara de este procedimiento podemos desarrollar el siguiente ejemplo. Imaginemos que pertenecemos a una red de 100 inversores. De esa red, existe un grupo de 50 inversores con 1000 monedas cada uno. Otro grupo de 30 inversores con 2500 monedas cada uno y un último grupo con 20 inversores con 10000 monedas cada uno.

Imagen 2. Ejemplo reparto de participación en la red

GRUPO DE INVERSORES	INVERSORES	MONEDAS EN RESERVA	TOTAL MONEDA DE RESERVA	% PARTICIPACIÓN
GRUPO A	50	1,000	50,000	15.38%
GRUPO B	30	2,500	75,000	23.08%
GRUPO C	20	10,000	200,000	61.54%
TOTAL	**100**	**325,000**	**325,000**	**100.00%**

Fuente: AcademyBit2me

Así, vemos que el grupo C es que más participación tiene en la red. En este momento se produce la selección aleatoria en la red, lo que significa que aquellos que tienen mayor participación son los que tienen mayor probabilidad de ser seleccionados. Esta mayor probabilidad no significa que los miembros del grupo A y B no vayan a ser elegidos, por lo que la mayor participación no garantiza que vaya a ser seleccionado como un nodo. Una vez que se han seleccionados los nodos, los inversores tienen la capacidad de realizar las tareas que se les proponen (las cuales radican en validar transacciones o crear nuevos bloques) con el fin de recibir incentivos y ganancias proporcionales a su participación. Finalizada la ronda, el proceso de selección comienza de nuevo con el fin de que otros inversores puedan participar. Este procedimiento, a diferencia del Proof of Work no precisa de tanta energía, lo que ha supuesto que muchos proyectos de blockchain se interesan por este nuevo protocolo.

2.1.5. LA FINANCIACIÓN A TRAVÉS DE LAS CRIPTOMONEDAS (ICO)

Cuando hablamos de ICO, la mayoría de las personas lo identifican con aquellas ayudas que ofrece el gobierno de España a emprendedores y empresas para llevar a cabo nuevos proyectos. Pero, pese a que existe coincidencia en la denominación, ICO en el mundo de las criptomonedas difiere sustancialmente de esas ayudas. Podríamos asimilarlo como una salida a bolsa, pero sin las restricciones establecidas en el OJ. ICO (Initial Coin Offering u Oferta inicial de monedas) en el ámbito del blockchain consiste en obtener financiación a través de la venta de una criptomoneda. Mediante este medio, las empresas

y personas obtienen una financiación instantánea (a diferencia de los préstamos o créditos tradicionales).

Se trata de una forma novedosa de recaudar dinero para las empresas emergentes. Podríamos decir que las ICO de criptomonedas están a mitad de camino entre el crowdfunding[13] y una salida a bolsa. Así, se venden tokens (unidades de la criptomoneda que se pretende desarrollar mediante el proyecto financiado) a cambio de dinero fiat (dólares o euros) o de otras criptomonedas como puede ser el Bitcoin. En términos más sencillos podríamos decir que las ICO son formas de financiación de proyectos (cuando digo proyectos me refiero a la creación de una nueva criptodivisa) mediante la cual se ofrecen monedas del proyecto que se pretende desarrollar a cambio de recursos que permitan llevar a cabo ese proyecto. Por ejemplo, imaginemos que queremos crear una criptomoneda, pero necesitamos recursos para ello. Para ello, pondríamos a la venta cierta cantidad de esta moneda (todavía no está en circulación) que estamos creando a cambio de recibir dinero u otra criptomoneda (como el Bitcoin). Los inversores nos comprarían estas cantidades de moneda que hemos puesto a la venta. Con esos recursos financiamos nuestro proyecto y lo llevamos a cabo. En el caso de que no se obtuvieran los recursos necesarios para llevar a cabo el proyecto se devolvería a los inversores sus aportaciones. Todo ello se lleva a cabo a través de Smart Contracts o Contratos Inteligentes.

El origen de las ICO se remonta a 2014, con la aparición de Ethereum. La estrategia de Ethereum fue de crear (o minar) la moneda por adelantado, pero sin llegarlas a poner en funcionamiento[14]. Es decir, pusieron a la venta las monedas antes de que el proyecto estuviera en funcionamiento. Como consecuencia de ello, obtuvo la financiación necesaria (19 millones de dólares en bitcoins) para desarrollar el trabajo que tenían que realizar posteriormente.

Ya en 2015, Ethereum decide la publicación de su software funcional desencadenando los Smart Contracts[15] o contratos inteligentes. La aparición de este tipo de contratos ha

[13] Consiste en recaudar pequeñas cantidades de dinero procedente de muchas personas para financiar un proyecto o empresa

[14] Esta estrategia se denomina en el mundo de las criptodivisas como "preminar" el cual consiste en crear una criptomoneda, pero no ponerla en funcionamiento, sino que se guarda o se pone a la venta para obtener financiación, pero la moneda no está funcionando en el criptomercado.

[15] Contratos escritos como un programa informático en lugar de en un documento impreso con lenguaje legal y cuya ejecución se realiza por sí misma.

habilitado la creación de nuevas criptodivisas sobre criptodivisas ya existentes. Es decir, derivados de monedas como Bitcoin o Ethereum. Como consecuencia de ello, el volumen de ICO en el mundo del blockchain ha sido impresionante.

Algo sorprendente de este fenómeno es que cualquier persona puede desarrollar una ICO de criptomonedas. Consiste en la emisión de un determinado número de tokens[16] poniéndolos todos, o algunos, a la venta. Encontramos otra ventaja importante. En caso de que la ICO no obtenga el dinero mínimo que se ha marcado para recaudar y financiar el proyecto, éste se cancela y se devuelve la cantidad correspondiente a los inversores. En caso de que se obtenga el dinero que se ha marcado como objetivo, éste será utilizado para la financiación del proyecto. Una vez desarrollado el proyecto, se espera que exista un aumento de la valoración de los tokens (existirá mayor demanda, con un número limitado de tokens, derivará en mayor precio) para que sean vendidos por los inversores.

2.1.6. LOS MONEDEROS DE CRIPTOMONEDAS (WALLETS)

Como ya he indicado anteriormente, las criptomonedas se caracterizan por no tener un soporte físico, sino que son monedas digitales en su totalidad las cuales funcionan por medio de la criptografía. Es este hecho el que otorga la gran importancia que tienen los monederos de criptomonedas para poder gestionar los fondos que tienen los particulares. Pero, en realidad, estos monederos no almacenan las criptomonedas como si fuera una cartera de dinero físico, sino que almacenan las claves públicas y privadas. Las criptomonedas no existen como monedas, sino que existen como una serie de registros de transacciones almacenados dentro de una blockchain y que, además, basa su operación en nodos interconectados entre sí. Pues bien, esas claves públicas y privadas de los monederos son las que van a permitir a los particulares obtener la propiedad de las criptodivisas que son transferidas a una dirección determinada.

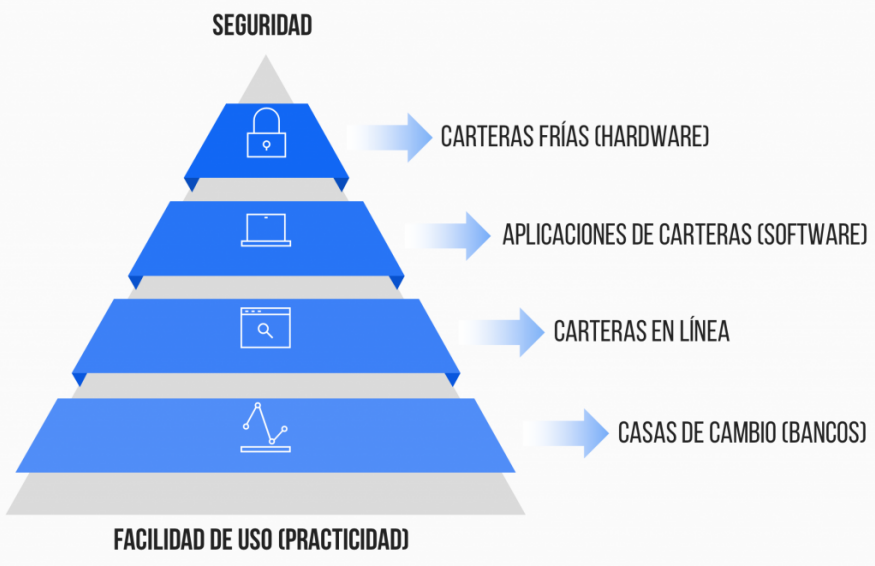
La clave pública es muy similar al número de cuenta bancario que todos conocemos. A través de ella, el tenedor de esta clave puede recibir fondos de otra persona además de tener la facultad de consultar el estado de los fondos. En lo que respecta a la clave privada,

[16] *"Los tokens son objetos similares a las monedas, pero estos carecen de valor de curso legal. Esto se debe a que los tokens son emitidos por una entidad privada para un determinado uso y en su elaboración normalmente se hace uso de materiales de escaso valor" – Bit2academy.*

podríamos asimilarla a una contraseña. En esta última clave es de vital importancia que el tenedor de la misma no la comunique a nadie ya que, aquel que tenga esta contraseña será el propietario de los fondos de la cartera y tendrá el control de los mismos.

En este punto, debemos resaltar la importancia que tienen las carteras o "wallets" en el mundo de las criptodivisas. Como las criptomonedas son sistemas que se encuentran totalmente descentralizados, no existe una entidad que las controle. Como consecuencia de ello, las carteras son el medio que va a permitir operar y consultar el saldo disponible de este tipo de activo. Al tratarse de un sistema descentralizado, no es preciso la autorización por parte de ningún agente externo para realizar operaciones. Por todo ello, es de vital importancia elegir adecuadamente la cartera, concretamente elegir aquella cartera que satisfaga las necesidades del tenedor de la mejor manera entre los tipos disponibles. Para clasificar los distintos tipos de carteras disponibles se utilizan dos variables, facilidad de uso y seguridad.

Imagen 3. Tipos de carteras o "wallets" disponibles



Fuente: Criptonoticias

Como podemos observar en el gráfico, existen cuatro tipos de carteras disponibles: Carteras frías (Hardware), Aplicaciones de carteras (Software), Carteras en línea y Casas de cambio (Bancos). En el *Anexo 2* se presenta el análisis de cada tipo de cartera, desde la punta de la pirámide hasta la base, es decir, desde aquellas carteras más seguras hasta las que son más fáciles de usar.

2.1.7. REGULACIÓN LEGAL DE LAS CRIPTOMONEDAS

Las criptomonedas ostentan entre sus características esenciales la desregularización, es decir, actualmente no existe ninguna norma de rango normativo que regule las criptomonedas en todos sus aspectos, únicamente consultas sin rango normativo. El problema principal con el que se encuentran los estados en la dificultad para definir las monedas virtuales. Las monedas virtuales son de reciente creación lo que supone la imposibilidad, o difícil subsunción de la figura en las categorías jurídicas tradicionales. Por ello, existe un gran debate sobre la naturaleza jurídica de las criptomonedas. La Directiva UE 2018/843[17] por la que se modifica la Directiva 2015/849 relativa a la prevención de la utilización de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE establece una definición de monedas virtuales como una *"representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos"*.

Pese a esta definición proporcionada por la directiva, no existe unicidad en la naturaleza jurídica de las criptomonedas. Desde un punto de vista económico, las monedas virtuales no reúnen las características clásicas de las monedas fiduciarias (medio de cambio, unidad de cuenta y depósito de valor). Tampoco deben confundirse con el dinero electrónico el cual es definido en el artículo 2.2 de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio) ya que el dinero electrónico es un mecanismo de transferencia digital de moneda. Con el dinero electrónico la relación entre el dinero tradicional y el electrónico tiene una base legal, y los fondos almacenados en la misma en la misma unidad monetaria, hecho que no se da en el caso de las criptomonedas. Desde el punto de vista legal, las criptomonedas ostentan propiedades tanto de moneda como de activo y medio de pago. Ello dificulta, como he indicado, su encuadre dentro de una regulación específica.

[17] https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32018L0843

Mientras que en EE. UU. encontramos una cierta regulación de las criptomonedas, en el ámbito comunitario y español carecemos de ésta.

La unidad de inteligencia financiera estadounidense (FinCEN) considera las monedas virtuales como una moneda en sí aunque no tiene todos su atributos, el regulador financiero estadounidense (SEC) considera las criptomonedas como un contrato de inversión de forma que son consideradas como instrumento financiero y el regulador del mercado de futuros (CFTC) les otorga la consideración de "commodity". A nivel comunitario, ha habido numerosos posicionamientos por parte de organismos como el Banco Central Europeo, la Autoridad Bancaria Europea, la Autoridad Europea de Valores y Mercados, pero la única regulación positiva es la que encontramos en la Directiva 2018/843. En el caso español más de lo mismo, no encontramos norma de derecho positivo alguna que aborde la regulación de un fenómeno que sigue creciendo a pasos agigantados. Únicamente podemos encontrar documentos sin rango normativo como consultas de la Dirección General de Tributos (DGT), avisos de la Comisión Nacional del Mercado de Valores (CNMV) y del Banco de España (BdE) o alguna resolución judicial como la sentencia de AP de Asturias de 6 de febrero de 2015 (Menéndez, 2018)[18].

En este sentido, la 5ª Directiva (UE) 2018/843 establecía como plazo máximo el pasado 10 de enero de 2020 para que los Estados Miembros adaptaran sus disposiciones legales, reglamentarias y administrativas para dar cumplimiento a lo establecido en la directiva. Cumpliendo con está obligación, el pasado 13 de octubre de 2020 el Consejo de Ministros de España aprobó el proyecto de ley denominado "Ley de Medidas de Prevención de Lucha contra la Elusión Fiscal". Con esta ley se pretende establecer controles estrictos sobre el uso de las criptomonedas con el objeto de evitar el fraude fiscal. Así, cualquier ciudadano español que opere con criptomonedas deberá comunicarlo de igual forma que si lo realizara con pagos en efectivo, es decir, cualquier tipo de pago que se realice con criptomonedas deberá ser declarado de la misma forma que lo es el pago con divisas.

[18] URÍA MENÉNDEZ. *"Monedas virtuales. Aproximación jurídico-tributaria y control tributario"* En *Actualidad Jurídica Uría Menéndez.* 2018.

En definitiva, las criptomonedas son un fenómeno que ha llegado para quedarse. Por ello, debe regularse de forma estricta tanto su funcionamiento como su consideración jurídica con el objeto de otorgar una protección a los usuarios que realicen transacciones con estas. A mi modo de ver la regulación de las criptomonedas a través de la Ley de Medidas de Prevención de Lucha contra la Elusión Fiscal es una noticia positiva con el objeto de evitar el blanqueo de capitales o la realización de actividades ilícitas a través de las criptodivisas. Ahora bien, creo sinceramente que se debe hacer un esfuerzo sustancial que lleve a la determinación clara de la naturaleza jurídica y regular todos los posibles aspectos en los cuales las criptomonedas pueden tener incidencia.

2.2. EL BITCOIN

2.2.1. ORIGEN Y CREADOR

El Bitcoin fue la primera criptomoneda en crearse, lo que la dota de especial importancia. Para encontrar sus orígenes debemos remontarnos al año 2008. Como bien sabemos, el año 2008 fue un año gris para las economías mundiales. Como consecuencia de la recesión mundial, la Federal Reserve Board[19] implementó políticas monetarias con el objeto de iniciar una recuperación económica progresiva. Es en este punto donde adquiere sentido el origen del bitcoin. El propósito de esta criptomoneda era la de crear una moneda que no estuviera controlada por las autoridades monetarias. Es lógico, por tanto, que ante un escenario donde imperaba una crisis económica de dimensiones no recordadas desde el crac del 29, apareciera el Bitcoin y no en otro momento. Por tanto, la aparición de esta moneda virtual en el año 2008 no es casualidad ni mucho menos.

Así, Bitcoin surge en el año 2008 con el propósito de otorgar a los ciudadanos la posibilidad de realizar transferencias de valor inmediatas, con un coste prácticamente nulo y que no pueda ser controlado ni por gobiernos ni por bancos.

El Bitcoin está basado en un modelo operativo descentralizado de forma que la emisión del mismo y el registro de los movimientos que se producen con ellos no va a ser controlado por ninguna autoridad. En lugar de ello, esta criptodivisa se basa en la red

[19] La Federal Reserve Board (FED) es el banco de la Reserva Federal el cual se encarga de la estabilidad financiera y monetaria de Estados Unidos.

P2P. La red P2P o "red entre iguales" es una red de nodos que se comportan de igual manera entre ellos de forma que actúan al mismo tiempo como servidores y como clientes respecto al resto de nodos. Es decir, en este tipo de redes los nodos se encuentran interconectados en una red de forma que comparten, entre los integrantes de la red, archivos almacenados en los discos duros de cada uno de ellos. Mediante el uso de una serie de aplicaciones específicas que permiten compartir los datos entre los citados integrantes, los usuarios pueden llevar a cabo consultas a otros nodos con el objeto de localizar y descargar archivos. Es en este punto donde podemos determinar la diferencia entre la actuación como cliente o como servidor. Así, en el caso de que un nodo descargue archivos de otros nodos de la red, actuará como cliente. Por el contrario, si un nodo es la fuente de la que los otros nodos descargan los archivos, actuará como servidor.

"Satoshi Nakamoto" es el conocido como creador del Bitcoin. Su identidad es un misterio ya que el citado nombre es un pseudónimo. Actualmente no se conoce con certeza quien puede estar detrás de la creación de la moneda más importante dentro del mundo de las criptomonedas. La única información acerca del creador del Bitcoin se obtiene a través de los datos publicados por el portal *P2Pfoundation:* se trata de un hombre de nacionalidad japonesa y de alrededor de unos 40 años. "Satoshi Nakamoto" anuncia el 1 de noviembre de 2008 en la lista de correo [20] "cryptography" [21] que había estado trabajando en un sistema nuevo de dinero electrónico donde resumía sus propiedades y su funcionamiento. Tres meses después, el 11 de febrero de 2009, a través del portal P2Pfoundation publicó un mensaje donde daba a conocer el portal oficial de Bitcoin, sus características fundamentales, el diseño y hasta el cliente inicial con el que comenzar a participar en la red. Ya en 2011, Satoshi Nakamoto se desvincula totalmente del proyecto, comunicándolo a través de un correo electrónico enviado a uno de los desarrolladores de Bitcoin.

[20] Función del correo electrónico que habilita el envío de mensajes entre múltiples usuarios que se encuentran inscritos en ella de forma simultánea.
[21] Se trata de una lista de correo denominada "cryptography" donde todos los usuarios inscrita a ella recibieron el correo electrónico de Satoshi Nakamoto donde se explica el origen el Bitcoin.

2.2.2. CONSIDERACIÓN COMO DIVISA O COMMODITY

Antes de comenzar a determinar si el Bitcoin es una divisa o un commodity, debemos definir qué se entiende por divisa y qué se entiende por commodity. Por definición, *"Una divisa es toda moneda extranjera, es decir, monedas oficiales distintas de la moneda legal en el propio país"* (Pedrosa, 2020) [22]. Una moneda es dinero de curso legal emitido por los bancos centrales de los países que tienen la función principal de servir de medio de pago para cualquier transacción. Por tanto, si entendemos que el Bitcoin es una divisa debería de cumplir esa función esencial de servir como medio de pago para cualquier transacción, independiente del hecho que ya conocemos de que las criptomonedas no son emitidas por los bancos centrales, pues están totalmente descentralizadas.

Las commodities por su parte son definidos por D. José Luis Caballero en su artículo de "El Economista" como un producto o bien por el que existe una demanda en el mercado y se comercian sin diferenciación cualitativa en operaciones de compra y venta. Dice el citado autor que *"cuando se habla de commodities, se entiende que son materias primas o bienes primarios, que, al basarse en una calidad estándar mínima, no existe una sustancial diferencia entre los mismos*".

El Bitcoin es una moneda virtual[23] de reciente creación, de forma que existe gran controversia acerca de su clasificación como divisa o commodity ya que se pueden dar argumentos en ambas direcciones. El propósito en la creación del bitcoin radica en servir como alternativa a las monedas fiduciarias cumpliendo las tres funciones principales que tiene el dinero fiduciario: medio de pago, es decir, usar el dinero con el fin de realizar cualquier tipo de transacción; unidad de cuenta en el sentido de determinar el precio de los bienes y servicios; y depósito de valor, es decir, capacidad para que el valor de un capital se mantenga estable y por lo tanto se puedan llevar a cabo operaciones en el futuro. La concepción del bitcoin como medio de pago lo ratifica la STJUE de 22 de octubre de 2015 en el asunto C 264/14. Pero los bitcoins no son exactamente divisas, sino que se podrían definir como neodivisas tal y como indica el TJUE en su sentencia donde expresa

[22] PEDROSA, J. *"Divisa*" en https://economipedia.com/definiciones/divisa.html
[23] Una moneda virtual es definida por el BCE como una forma de dinero digital no regulado, no emitido ni garantizado por un banco central y que puede actuar como medio de pago.

que existen divisas tradicionales y no tradicionales, estando el bitcoin dentro de estas divisas no tradicionales.

Por otra parte, si consideramos la moneda virtual como commodity podemos encontrar ciertas semejanzas con el oro, pues ambos tienen el atributo de escasez. Tanto en el caso del oro como en el caso del Bitcoin se entiende que existe un número limitado de los mismos. Así, el oro se entiende que es limitado, y el bitcoin se prevé que existirá un máximo de 21 millones de monedas. Cuando se llegue a ese número de monedas, se dejarán de crear más. En este sentido, son numerosos los autores que consideran el bitcoin como un activo objeto de inversión puesto que los usuarios consideran el bitcoin como un activo de inversión altamente volátil y especulativo (Glaser, 2014 [24] . Como consecuencia del creciente interés de los usuarios por la citada criptomoneda como instrumento de inversión, ha sido reconocido como commodity virtual por organismos como la Commodity Futures Trading Comission[25] (CFTC) en Estados Unidos o por la Canada Revenue Agency (CRA).

Podemos colegir que el bitcoin tiene cabida tanto dentro de su consideración como divisa o como instrumento de inversión puesto que como he indicado anteriormente los consumidores pueden usarlas como medio de pago para sus transacciones (aunque su uso no está generalizado puesto que no existe confianza en este medio de pago) y como instrumento de inversión (los consumidores invierten en bitcoin con objeto de obtener una rentabilidad como consecuencia de las variaciones del precio del bitcoin); sería un híbrido entre el dinero y las materias primas como el oro. Esta es la concepción que le dan los usuarios al bitcoin. Pero las autoridades difieren en su consideración dependiendo de la ubicación geográfica donde se encuentre. Así, en EEUU es considerada como una commodity mientras que en la UE es considerada como una divisa. Por tanto, y aunque parezca irónico, no se puede dar una respuesta rotunda a si el bitcoin es una divisa o una commodity. En mi opinión, el Bitcoin debe considerarse como una commodity. Para que fuera considerada como una divisa debería de ser aceptada como medio de pago. Pese a que para determinadas transacciones se permite el pago en bitcoin, su uso no está

[24] GLASER, F., ZIMMERMANN, K., HAFERKORN, M., WEBER (2014) Bitcoin-asset or currency? Revealing users hidden intentions.
[25] La CFTC es la Comisión del Comercio en Futuros sobre materias primas de EEUU, constituyendo una agencia federal independiente del gobierno que regula los futuros de materias primas y el mercado de opciones.

generalizado. El bitcoin se usa principalmente como medio de especulación para obtener rentabilidades increíbles como consecuencia de su oscilación en los precios. Por ello, no creo que se pueda comparar la función del bitcoin con la del dólar o el euro, sino que sería más acertada considerarlo como una herramienta de especulación.

2.2.3. EL FENÓMENO HALVING

Como hemos indicado anteriormente, los mineros reciben unidades de bitcoin por cada bloque que crean dentro de la cadena de bloques. Así, y tal y como establece el propio software de bitcoin, cada vez que uno de los mineros vaya creando bloques mediante la validación de transacciones, éstos van a recibir bitcoins como recompensa por su trabajo. El halving es un evento mediante el cual esta recompensa en bitcoins se reduce a la mitad. Es decir, si antes un minero recibía 50 bitcoins por la creación de un bloque, ahora recibirá 25 bitcoins. La explicación de este evento radica en el hecho de que la cantidad de bitcoins que pueden llegar a existir está determinada desde la creación del bitcoin, concretamente la cantidad máxima de bitcoins en circulación es de 21 millones. Este proceso sirve para fichar un periodo de tiempo concreto para finalizar la emisión de bitcoin con el fin de que el valor de la moneda suba paulatinamente. Esto es, lo que se busca mediante este evento, es que no se produzca una rápida emisión de todas las monedas y por tanto puedan acabar todas en las manos de un solo individuo, sino que estén más repartidos. Pero los mineros, al recibir los bitcoins, no tienen en sí una recompensa económica. Únicamente tienen una moneda recién minada que necesita para adquirir valor ser intercambiada por un elemento de valor, como un dólar o un euro con el que pagarán los gastos de energía o de otro tipo en los que hayan incurrido para la generación de un bitcoin[26]. Ello es lo que es explica que a partir del halving, el precio del bitcoin suba. Si como consecuencia de la validación de transacciones y la creación de bloques los mineros reciben menos bitcoin, es lógico que retengan las monedas que tienen hasta que el precio de las monedas vuelva a subir y por tanto obtengan rentabilidad por la operación. Es decir, están reduciendo indirectamente la oferta de bitcoin, y siguiendo con las leyes de la oferta y la demanda, a menor oferta de un determinado bien, mayor precio.

[26] https://academy.bit2me.com/que-es-halving-bitcoin/

El halving sucede aproximadamente cada cuatro años o, en términos de bloques generados, cada 210.000 bloques. Así, el primer halving ocurrió el 29 de noviembre de 2012, el segundo el 10 de julio de 2016 y el tercero ha ocurrido recientemente, en mayo de 2020.

2.3. OTRAS CRIPTOMONEDAS. ALTCOINS

Como he indicado en el apartado anterior, el Bitcoin es la criptomoneda más importante dentro del mercado de las criptodivisas. Actualmente, el mercado de las criptodivisas no está formado únicamente por el Bitcoin, sino que ha ido evolucionando hacia monedas alternativas que reciben el nombre de "Altcoins". Los Altcoins se refieren a criptomonedas que derivan del código abierto del bitcoin, que no son bitcoin y que reúne en el mismo concepto tanto a criptomonedas como tokens. Estas monedas alternativas y tokens tienen por objeto, entre otros: servir de como elemento innovador en el sentido de solucionar problemas y mejorar aspectos del blockchain y del bitcoin; ofrecer facilidades a las empresas y los usuarios mediante la simplificación de los procesos de manufactura por ejemplo; por último, otro punto a destacar sería la descentralización, pero no en un sentido de que se traten de monedas que no sean emitidas por autoridades o bancos centrales, sino más bien en el sentido de evitar que todo el mercado de criptomonedas se centralice en un equipo, otorgando a usuarios que quieran participar la posibilidad de hacerlo (mediante la producción de monedas virtuales).

Ahora bien, es extremadamente difícil realizar una lista exhaustiva de las motivaciones que impulsan el desarrollo de las altcoins (aunque la mayoría de ellas comparten un motivo lucrativo). Así, cada uno de los altcoins que se crean pueden tener una finalidad distinta, por lo que voy a exponer los tres altcoins más importantes en términos de relevancia del proyecto que llevan a cabo. Dentro de las Altcoins se pueden diferenciar dos grupos: el primero que incluye criptomonedas que provienen de una bifurcación de bitcoin (por ejemplo, Litecoin, Dogecoin…); y un segundo grupo que han construido su propio blockchain, utilizando hasta algoritmos de minería diferentes al del bitcoin (Sánchez, 2018) [27]. El desarrollo de los tres Altcoins más importantes se encuentra en el *Anexo 3*.

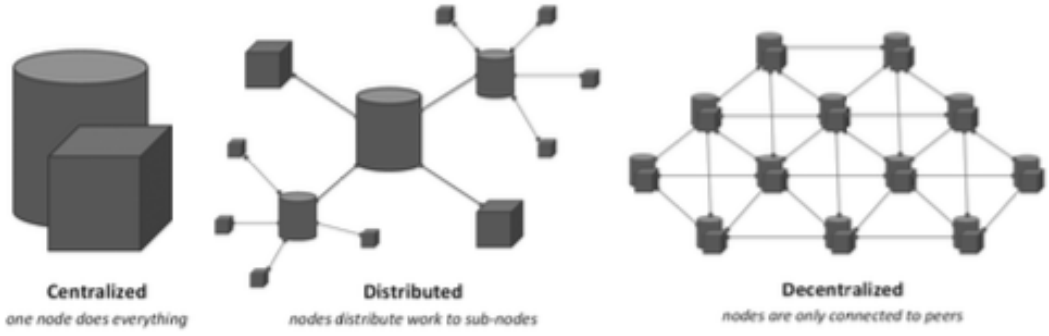
[27] SÁNCHEZ ROA, JULIA. "*Criptomonedas"* En https://www.pj.gov.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf

3. EL PROCESO DE NEGOCIACIÓN DE LAS CRIPTOMONEDAS Y DIVISAS.

3.1. MERCADO DE CRIPTOMONEDAS

Hasta la aparición de las criptomonedas, las organizaciones han hecho uso de bases de datos tradicionales con el objeto de registrar todas las transacciones e información. Siempre ha sido necesaria la existencia de un intermediario como una autoridad central, un banco o la oficina gubernamental con el objeto de que lleve a cabo las modificaciones de las transacciones, identificando quién posee qué en un momento dado. Hasta aquí parece que existen muchas similitudes entre las redes blockchain y las redes tradicionales en el sentido de registrar las transacciones y comprobar que el transmitente de una cosa es propietario de esta. Pero las redes tradicionales tienen un importante problema de ineficacia en cuanto a costes y tiempo, problemas que se solucionan con las redes blockchain. Las redes tradicionales, como he indicado, dependen de un único intermediario que es el que va a comprobar y autorizar la transacción mientras que en las redes blockchain, son todos los participantes de la red los que comprueban y autorizan la transacción de forma simultánea y a un coste prácticamente nulo. Además, las posibilidades de corrupción en las redes tradicionales son mucho más elevadas que en las redes blockchain puesto que en el primer caso depende únicamente de un ente, mientras que, en el segundo, si alguien intenta llevar a cabo una acción fraudulenta, tiene un ejército de nodos detrás con la copia original de la transacción, por lo que es prácticamente imposible (Parrondo, 2008)[28].

Imagen 4. Tipos de sistemas



Fuente: Mesh World P2P Simulation Hypothesis, Eric Grange

[28] LUZ PARRONDO, "Tecnlogía blockchain, una nueva era para la empresa". Revista de Contabilidad y Dirección. Vol. 27, año 2008, pp 12- 16

3.2. FUNCIONAMIENTO DEL MERCADO DE DIVISAS

En primer lugar, debemos definir qué se entiende por divisas. Las divisas son las monedas utilizadas en un país distinto de aquel de origen. Por ejemplo, en España, una divisa sería el dólar pues es una moneda diferente a la utilizada con carácter habitual en nuestro país (el Euro).

El mercado de divisas o FOREX (Foreign Exchange Market) es un mecanismo a partir del cual oferentes y demandantes de monedas extranjeras pueden intercambiar las mismas. De esta definición podemos vislumbrar la función principal del mercado de divisas, la cual consiste en realizar la conversión de una moneda a otra, estableciéndose un precio de intercambio. Lo que se pretende con estas conversiones de moneda es paralizar la operación hasta que se produzca un incremento en el valor de la moneda objeto de intercambio, de forma que se vuelve a cambiar por la de origen y se obtiene así beneficio.

Para saber cuanto vale una moneda, siempre la comparamos con otra divisa. Por ejemplo, si queremos saber cuánto vale el euro lo que se hace comúnmente es compararlo con el dólar americano. Este hecho es importante por ejemplo si necesitamos pagar en dólares algún bien o hacer turismo en el país estadounidense. Actualmente, un euro equivale a 1,21 dólares, por lo que en caso de que quisiéramos intercambiar 1000 euros, nos darían 1210 dólares. Pero mucha gente no conoce que se puede llevar a cabo una operación similar para intentar ganar dinero. Es decir, si como consecuencia de algún acontecimiento político o como resultado de llevar a cabo un análisis técnico creemos que el par EUR/USD va a subir, lo más adecuado sería comprar la divisa al precio de este momento, en nuestro caso actual a 1,21 dólares. Con ello se espera que 1 euro equivalga en el futuro a 1,24 dólares (por ejemplo) en el futuro, momento en el que se venderán los dólares que se tengan, obteniendo así un beneficio económico.

Para realizar esta operación, se hace uso del mercado FOREX, concretamente un bróker o intermediario fiable. Una característica esencial del mercado FOREX es que opera las 24 horas del día durante 5 días a la semana, siendo el mercado más líquido y con mayor volumen intercambiado, siendo la base para las transacciones internacionales de capital. Los pares de divisas más comercializadas y que representan más del 80% del comercio

total de divisas son las siguientes: EUR/USD, GBP/USD, USD/JPY, USD/CAD y AUD/USD. La moneda de la izquierda es la moneda principal o base, mientras que la moneda de la derecha es la moneda secundaria.

3.3. PRINCIPALES DIFERENCIAS

Las criptomonedas, como es obvio y he desarrollado a lo largo del trabajo, presentan unas características sustancialmente distintas a las monedas tradicionales. En este punto, pretendo resumir las principales diferencias entre las monedas tradicionales y las monedas virtuales a modo de resumen. Así, las monedas tradicionales son físicas, mientras que las criptomonedas son virtuales. En el caso de las monedas tradicionales se intercambia dinero para adquirir algo de valor, mientras que en el ámbito de las criptomonedas se intercambia valor en forma de criptomonedas. Las criptomonedas, como ya sabemos están descentralizadas, siendo controladas por todos los usuarios y la tecnología blockchain. En cambio, las monedas tradicionales son emitidas por el gobierno y controladas por los bancos centrales y reservas económicas. Además, el valor de las monedas tradicionales está muy influenciadas por la inflación y el tipo de interés, mientras que en la determinación del precio de las criptomonedas únicamente influye la oferta y la demanda. Por último, y como he indicado anteriormente, las monedas tradicionales suelen tener una comisión en cada transacción que se realiza con las mismas, mientras que las criptomonedas permiten realizar transacciones de manera instantánea y sin comisión alguna.

4. CRIPTOMONEDAS VS DIVISAS

Una vez realizada una aproximación teórica al mercado de divisas y a su utilización como medio especulativo, vamos a proponer un supuesto con el fin de concluir en qué mercado interesa más invertir, si en FOREX o en el mercado de las criptomonedas.

Imaginemos que tenemos 1000 euros para invertir, pero no sabemos si invertir en FOREX o en Bitcoin. Para ello, vamos a analizar cuál sería la decisión en el caso de que compráramos dólares a fecha 31 de diciembre de 2008 y los quisiéramos vender en enero de 2021. La cotización EUR/USD en 2008 era de 1,3917 dólares por cada euro, de forma que si hubiéramos comprado dólares hubiéramos obtenido 1391,7 dólares por los 1000 euros que teníamos. En el hipotético caso de que quisiéramos vender en 2021 estos dólares por euros, los resultados serían desastrosos, pues la cotización euro dólar es de 1,21. Ello conlleva que recibiríamos menos euros que los vendidos en el año 2008, una operación pésima para nuestros intereses. Además, en todas las operaciones de compra de divisas existen una serie de gastos y comisiones por parte de la entidad financiera a través de la cual realicemos la operación. Por ejemplo, si compráramos divisas a través de la entidad financiera BBVA, la comisión de apertura del contrato sería de un 3,33% sobre el nominal y la comisión de mantenimiento de un 1,57% sobre el nominal.

Una vez determinado el supuesto de inversión en el mercado FOREX, vamos a ver qué ocurriría si decidiéramos invertir esos 1000 euros del año 2008 en la compra de bitcoins. Por esos años, con el Bitcoin recientemente creado, éste no tenía valor alguno, simplemente algunos fans que lo intercambiaban en foros a modo de prueba. No es hasta 2010, cuando Laszlo Hayneck pagó dos pizzas por 10.000 bitcoins cuando esta moneda adquiere algo de valor (unos 0,003 dólares). Poco a poco el bitcoin fue adquiriendo importancia hasta que, en el año 2011 aumenta su precio alcanzando paridad con el dólar. Es decir, en el año 2011 una unidad de bitcoin era equivalente a un dólar. Así, en ese año si hubiéramos invertido los 1000 euros de capital que teníamos hubiéramos obtenido 773 bitcoins. Pero como bien sabemos, y he desarrollado a lo largo del trabajo el precio actual de esta criptomoneda dista en gran medida de esta valoración inicial. En el año 2021 el precio de 1 bitcoin es de 28.900 euros. Así, si quisiéramos vender los 773 bitcoins obtenidos en el año 2011 obtendríamos la escalofriante cantidad de 22.340.473 euros.

El Bitcoin, como ya he indicado anteriormente, tiene tres funciones principales: a) Consideración como medio alternativo de pago; b) Consideración como divisa; y c) Consideración como inversión. Considerar el Bitcoin como medio alternativo de pago no tiene cabida actualmente ya que existe una falta de confianza por parte de los consumidores para su utilización por este medio, además que no es admitido en la mayor parte de establecimientos. Considerar esta criptomoneda como divisa tampoco parece ser viable puesto que es una moneda extremadamente volátil. La práctica más extendida es considerar el bitcoin como un instrumento de inversión a partir del cual se pretende obtener rentabilidades derivadas de la compra y venta de esta moneda virtual.

Para una mayor precisión a la hora de seleccionar la inversión más favorable a nuestros intereses debemos utilizar la Tasa Anual Equivalente (TAE). Se trata de un instrumento financiero que recoge todos los términos de la inversión, tanto comisiones como el plazo de la inversión con el fin de otorgar un valor representativo del beneficio real de la operación. En el *Anexo 4* presento la evolución del ROI de ambas alternativas de inversión.

Veamos en primer lugar la TAE de invertir en el mercado FOREX. Realizamos una compra de dólares a fecha 1 de enero de 2020 en la entidad financiera BBVA que nos cobra una comisión de apertura de 3,33% sobre el nominal, así como un 1,57% sobre el nominal en concepto de comisión de mantenimiento. Así, en el momento de compra de USD se nos cobra una cantidad de 49,03€. Esta comisión la descontaremos al saldo final de la inversión. Una vez establecidas las comisiones veamos con mayor detalle la operación. Al adquirir USD el día 1 de enero de 2020 nosotros obtendremos 1.121,20 USD. Supongamos ahora que queremos vender esos dólares a fecha 8 de febrero de 2021. Como el tipo de cambio ha evolucionado, nosotros tenemos 1.204,70 USD. En ese momento el tipo de cambio EUR/USD es de 1,2047, por lo que las comisiones que tenemos que abonar en dólares ascienden a 59,06 USD. El capital resultante de la operación descontadas las comisiones son de 1.145,04 USD. Para el cálculo de la TAE debemos tener en cuenta el número de días que hemos mantenido la inversión, en el plazo propuesto es de 404 días. Por tanto:

$$\text{Interés diario} = (1.145{,}04/1.121{,}20)^{(1/404)} - 1 = 0{,}005208\%$$

Anualizando el interés diario obtendremos la TAE de la inversión. Es decir,

$$TAE = (1+0{,}00005208063)^{365} - 1 = 1{,}9191\%$$

Vamos a realizar ahora el cálculo de la TAE para la inversión en Bitcoin en el mismo periodo que hemos considerado para el cálculo de la TAE en el caso de los dólares. Para el cálculo de esta supondremos que utilizamos la aplicación CoinBase, la cual te permite adquirir criptomonedas mediante transferencia bancaria o tarjeta de crédito. Seguimos con las mismas consideraciones iniciales (capital inicial de 1000€ y compra del activo a fecha 1 de enero de 2020). La mencionada aplicación te cobra una comisión del 3,5% sobre el capital invertido, por lo que en nuestro caso deberemos abonar 35€ en concepto de comisión de apertura, y una cantidad fija de 2,97€ por la retirada de fondos. En el momento inicial de la inversión adquiriremos 0,16 Bitcoin (el precio del Bitcoin a esa fecha era de 6.410€) o en términos equivalentes 1000€. El día 8 de Febrero de 2021 el precio del Bitcoin ascendía a 35.540,40€. Por lo tanto, si vendiéramos en ese momento nuestra cantidad de monedas, obtendríamos 5.544,35€. A esta cantidad debemos de restarle las comisiones mencionadas anteriormente, de forma que el capital neto resultante de la inversión ascendería a 5506,38€. Procedemos a calcular la TAE siguiendo la misma operativa que la utilizada en el caso de la inversión en USD.

$$\text{Interés diario} = (5506{,}38/1000)^{(1/404)} - 1 = 0{,}423147\%$$

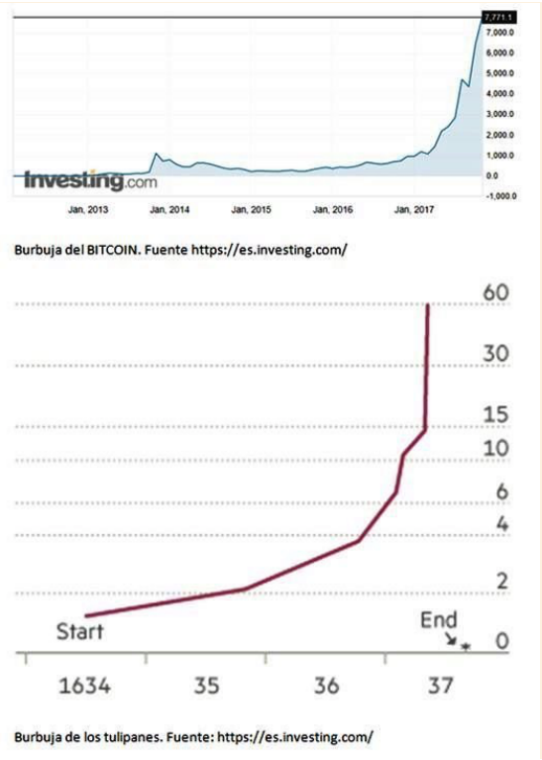
Anualizando el interés diario obtendremos el TAE de la inversión en Bitcoin. Así,

$$TAE = (1+0{,}00423147)^{365} - 1 = 367{,}0319\%$$

Vemos por tanto la increíble rentabilidad que nos otorga la inversión en la mencionada criptomoneda en comparación con la inversión en el mercado FOREX. Una rentabilidad excepcional que nos lleva a introducir el siguiente punto, relativo a la posibilidad de considerar el bitcoin como una "burbuja financiera", comparable con otras burbujas que han tenido lugar a lo largo de la historia como la "crisis de los tulipanes".

En el siglo XVII, en Holanda, los tulipanes llegaron a ser muy cotizados. Rápidamente se convirtieron en un codiciado objeto de lujo. Se compraba un tulipán, pero no físicamente, sino a través de un papel que le proporcionaría un bulbo a comienzos de la primavera siguiente. La gente hipotecaba sus casas por invertir en tulipanes, llegando una determinada especie a costar 6.000 florines (en el siglo XVII una persona normal en los Países Bajos tenía unos ingresos medios anuales de 150 florines). Hasta que este mercado explotó como consecuencia de que todos querían vender y nadie quería comprar. La gente compraba tulipanes para obtener una rentabilidad derivada de su venta, pensando que el precio de los mismo crecería más y más. Parece bastante semejante al fenómeno bitcoin actual.

Imagen 5. Burbuja Bitcoin y Burbuja de los tulipanes



Fuente: Expansión

Actualmente, el Bitcoin es la criptomoneda más conocida. Todo el mundo quiere invertir en Bitcoin como consecuencia de los constantes incrementos en los precios que se han producido desde su aparición, derivando en una rentabilidad tan grande que ningún instrumento financiero es capaz de proporcionar. El problema fundamental es que la gente invierte sin saber qué es una criptomoneda, qué variables determinan el cambio en su precio y cuál es la evolución que se espera de ella. Lo dejan todo en manos del azar. Este

es un riesgo puesto la gran cantidad de demanda de bitcoin hará, en mi opinión, que en el momento de vender esta moneda nadie quiera comprarla. No es una visión a corto plazo, es decir, creo que el bitcoin puede incrementar su precio mucho más. Es más, en palabras de Luis Ferruz: *"¿Quiere todo esto decir que el Bitcoin no puede subir más? ¡Claro que no!, los tulipanes pasaron de 1 florín a 60 en poco tiempo. Si consideramos que la burbuja del bitcoin empieza en 2017, sólo ha multiplicado por 10. Y según lo que ocurrió con los tulipanes podría todavía triplicar su precio".*

Siguiendo con el planteamiento inicial sobre si decidir invertir en bitcoin o invertir en divisas creo que la respuesta es clara en términos de rentabilidad. Si invertimos en divisas la rentabilidad es extremadamente menor que si invertimos en bitcoin (viendo la evolución de los precios). Pero no hay que tener en cuenta sólo la rentabilidad como aspecto clave para tomar esta decisión. Existen otros aspectos como podrían ser la aversión al riesgo del potencial inversor. Así, un inversor muy averso al riesgo no invertiría en bitcoin ya que el riesgo de perder tu capital es elevado como consecuencia de la gran volatilidad de los precios y de la incertidumbre sobre la evolución de los mismos. Otro aspecto sería la falta de confianza de las criptomonedas en el público en general. De esta forma, la falta de regulación puede llevar problemas derivados de fraudes o estafas en este ámbito que puede llevar a un potencial inversor a declinar la opción de invertir en bitcoin.

Por último, me gustaría indicar la capacidad económica de un inversor. Una de las claves para invertir, es invertir aquello que no necesites. ¿Qué quiere decir esto? Debes invertir una cantidad de dinero que no comprometa (en caso de pérdida) las posibilidades de satisfacer tus necesidades básicas. Así, un inversor que tenga muchos recursos económicos puede ser que decida invertir en ambos mercados puesto que no tienen problemas de limitación de capacidad financiera, mientras que uno cuyo presupuesto sea más ajustado debe decidir si invertir en un mercado o en otro. Ya para finalizar, creo que el momento actual es un buen momento para invertir en bitcoin puesto que las expectativas del precio siguen siendo alcistas (recientemente Bitcoin ha alcanzado su máximo histórico con un valor de 39.980€). Ahora bien, es necesario ser prudente y saber cuando debes salir del mercado, esto es, cuando deberías vender tus reservas de bitcoin (puesto que considero que es una burbuja que explotará en un momento futuro de la historia).

Para un mayor contraste en la formación de la burbuja especulativa que está ocurriendo alrededor de Bitcoin, adjunto una ilustración donde se describen las fases de formación de una burbuja. Así, podemos ver cuatro fases claramente diferenciadas. En primer lugar, la fase oculta que ocurre cuando el valor del activo, en este caso el Bitcoin, es reducido, su uso poco extendido y su conocimiento nulo. Una segunda fase, denominada "fase de conciencia" que tiene lugar cuando el activo se va dando a conocer entre los usuarios y su demanda es mayor. Este incremento en la demanda supuso el incremento del precio del Bitcoin.

A partir de la tercera etapa es cuando se empieza a formar la burbuja, el valor del activo empieza a crecer cada vez a mayor velocidad, las expectativas de rentabilidad son altas y entran en juego los pequeños inversores. La última etapa es la denominada "fase de hundimiento" que tiene lugar cuando una burbuja explota, es decir, se producen resultados menores de los esperados, los inversores quieren vender y el activo pierde valor. Con el Bitcoin estamos en entre la etapa de toma de conciencia y manía. El valor de esta criptomoneda no deja de subir, pese a su alta volatilidad, lo que está llevando a que muchísima gente sin ningún tipo de conocimiento sobre la inversión en criptomonedas empiece a invertir. Este hecho hace que el precio suba cada día más (sobre todo después del reciente halving que se produjo en mayo del año 2020).

Imagen 6. Fases en la formación de una burbuja especulativa.

Fuente: Rankia.com

En definitiva, como ya he indicado anteriormente, en términos de rentabilidad está claro que lo más adecuado es invertir en Bitcoin. Sin embargo, creo que es una burbuja que explotará dentro de un tiempo, por lo que se debe tener en cuenta este riesgo y saber cuando es el momento más adecuado para vender la cantidad de bitcoins adquiridos.

Para finalizar este punto presento una comparativa de la evolución de los precios de las tres criptomonedas más importantes en términos de capitalización bursátil en el periodo concerniente entre el 15 de enero de 2018 hasta la actualidad. Del estudio de este gráfico veremos la increíble tendencia alcista del Bitcoin, así como la conveniencia de invertir en Bitcoin si queremos obtener una rentabilidad excepcional (teniendo en cuenta todo lo que he expuesto con anterioridad sobre su riesgo).

Imagen 7. Comparativa precios LTC/BTC/ETH

Fuente: Investing.com

- La línea roja representa la evolución del precio del Bitcoin en periodo analizado. Un incremento en su precio de un 264,79% avala la hipótesis de tratarse de una burbuja especulativa.
- La línea negra representa la evolución del precio de Ethereum. Pese a ser la segunda criptomoneda de la historia y la segunda en términos de capitalización bursátil del mercado de las criptomonedas, no representa una tendencia similar al Bitcoin. Observamos que su precio ha caído un 20,21% desde enero de 2018. Ahora bien, debemos indicar que la oscilación de su precio a lo largo del periodo no es muy pronunciada. Es decir, su volatilidad (y por tanto su riesgo) es bastante más reducida que en el caso del Bitcoin. Pese a ello, su evolución tiene tintes de burbuja especulativa si vemos el impresionante incremento de precio desde su origen.
- La línea azul representa la evolución del precio de LiteCoin. LiteCoin, como he indicado anteriormente, es considerada la plata de las criptomonedas. Se trata de una criptomoneda íntimamente ligada con el Bitcoin, lo que justifica el incremento en el precio que se ha producido en los últimos años. Tal y como sucedía con Ethereum la volatilidad con respecto al Bitcoin es realmente reducida.

Así, la decisión sobre si invertir en una criptomoneda u otra es una decisión realmente personal. Una persona realmente aversa al riesgo quizá se decante más por el LiteCoin pues es la criptomoneda que más estabilidad presenta. Sin embargo, el Bitcoin siempre será la mejor opción en términos de rentabilidad. Veremos cómo evoluciona el mercado de las criptomonedas y la regulación que puedan hacer de ellas los gobiernos de los países. Creo que si se empieza regular las criptomonedas su valor descenderá estrepitosamente. Ello, unido a la clara existencia de una burbuja especulativa, llevará a grandes pérdidas de los inversores. Por ello, y como ya he indicado, un aspecto clave en la inversión de criptomonedas es invertir aquella cantidad de dinero que no comprometa tu capital pues es un mercado tremendamente desconocido y no sabemos con certeza qué dirección va a tomar.

5. CONCLUSIONES

La aparición del mercado de las criptodivisas ha supuesto una verdadera revolución en el sistema tradicional de pagos. Hace 30 años era inimaginable que fuera a existir una moneda descentralizada como el Bitcoin. Desde 2017 su popularidad ha ido creciendo exponencialmente. Bitcoin es la primera criptomoneda, y por ello, la más importante. Con su proliferación se pretendía crear un nuevo modelo de pago mundial que sustituyera las divisas tradicionales y las entidades que se encargan de emitirlas.

La revolución tecnológica que hemos vivido en la última década ha dotado de mayor importancia a este sistema alternativo de pago. En los últimos años, las empresas y los bancos han dirigido sus acciones hacia una sustitución del dinero en efectivo hacia sistemas de dinero digital. Así, han aparecido las tarjetas de crédito con sistemas contactless, aplicaciones para operaciones a distancia como puede ser PayPal o interfaces para potenciar las ventas online como Amazon, pero estos sistemas en nada se parecen al blockchain y las criptomonedas (salvo que son medios digitales).

No es hasta 2008 cuando aparece la primera criptomoneda, el Bitcoin. La gran recesión a la que se vio sometida la economía mundial, unido a la desconfianza de la ciudadanía en los bancos y los gobiernos constituyeron un escenario ideal para la proliferación de un sistema alternativo de pagos que no dependiera de ninguna autoridad gubernamental. Sin embargo, y pese a que el fin inicial de las criptomonedas era sustituir los medios tradicionales de pago, no ha adquirido esta naturaleza ni mucho menos. Las criptomonedas se han convertido en un medio alternativo de inversión, un medio especulativo de popularidad creciente.

El fin esencial de este TFG era desarrollar una explicación detallada del funcionamiento del mercado de las criptodivisas, dar una visión clara y sencilla que permitiera a los potenciales lectores comprender qué es eso de las criptomonedas de lo que todo el mundo habla. Además, los medios tradicionales de inversión son ampliamente conocidos (bonos del estado, acciones, FOREX…) por lo que ante el creciente interés de la sociedad en invertir en estas monedas virtuales propongo mi opinión acerca de la inversión en este activo. Hemos llegado a la conclusión de que las criptomonedas, en concreto en Bitcoin, no pueden considerarse como una divisa ya que no está generalmente aceptada como

medio de pago (si bien es cierto que se está empezando a admitir, como en el caso de Tesla la cual anunció recientemente que aceptará pagos en esta divisa digital[29]).

Una de las características esenciales de las criptomonedas es su desregularización. Creo y deseo que ocurra en un corto periodo de tiempo, que las criptomonedas deben ser objeto de regulación legal (sobre todo en marco de la UE). El Bitcoin es una criptodivisa muy usada y el hecho de que exista ausencia de regulación hace que muchos usuarios no tengan la suficiente confianza como para usarla como medio de pago. Una regulación legal opino que sería esencial para que el Bitcoin consiguiera su propósito inicial, es decir, lograría convertirse en un método alternativo de pago y no en un mero instrumento especulativo.

La parte empírica del TFG ha sido centrada en decidir en qué mercado interesaría invertir ante dos alternativas: el mercado de criptodivisas y el mercado de divisas (FOREX). Como he concluido en el apartado correspondiente, en términos de rentabilidad es inmutable el hecho de que es más interesante invertir en el mercado del blockchain. Ahora bien, es evidente que estamos ante una burbuja especulativa que mucho se parece a otras burbujas que se han producido a lo largo de la historia (crisis de los tulipanes, boom inmobiliario…). Es muy importante ser prudente con este tipo de inversiones que aportan una gran rentabilidad a corto plazo, pero llevan ligado un riesgo francamente mayor.

Si por algo se caracteriza el precio de las criptodivisas es su alta volatilidad, ello unido a mi percepción de que la burbuja explotará, no creo que sea un medio seguro donde invertir tu capital. Y nos preguntaremos ¿cuándo explotará esta burbuja? No creo que vaya a ser un hecho muy lejano. Hemos dicho que la cantidad máxima prevista de Bitcoins en circulación es de 21 millones (actualmente hay alrededor de 19 millones). Expertos en la materia consideran que el último bloque de Bitcoin se minará aproximadamente en el año 2140. Cuando no se produzcan más unidades de Bitcoins, su precio va a depender de la oferta y la demanda (ocurre ya ahora este hecho, pero con los halving tienen un impacto importante en el precio). En ese momento es donde se verá si el Bitcoin es un buen activo para invertir. En mi opinión, a partir de ese momento todo el mundo querrá vender su

[29] Tesla compra 1.250 millones en bitcoins y dispara la criptomoneda. https://www.lavanguardia.com/economia/20210209/6232872/tesla-compra-1250-millones-bitcoins-dispara-criptomoneda.html

cantidad de criptodivisas que tengan en su wallet lo que derivará en la esperad explosión de la burbuja especulativa. La experiencia avala que todas las burbujas especulativas han explotado, y creo que ésta no va a ser menos.

En definitiva, el gran desafío que plantea la revolución del Blockchain y las criptomonedas no tienen un futuro certero. Como medio especulativo, creo que el futuro es pésimo. Ahora bien, como sistema alternativo de pagos no ya que sustituya, sino que complemente a las divisas tradicionales puede ser un fenómeno muy interesante siempre y cuando las autoridades empiecen a mostrar interés en regular este novedoso sistema.

6. BIBLIOGRAFÍA

Arroyo Guardeño, D. (2019) *¿Qué sabemos de Blockchain?* Madrid.

Boucher, P. (2017). *How blockchain technology could change our lives. In-depth Analysis.* European Parliamentary Research Service.

Champagne, P. (2014) *El libro de Satoshi.* En *La colección de escritos del creador de Bitcoin Satoshi Nakamoto*.

Uría Menéndez. (2018). *Monedas virtuales. Aproximación jurídico-tributaria y control tributario.* En *Actualidad Jurídica Uría Menéndez.*

Glaser, F., Zimmermann, K., Haferkorn, M., Weber (2014). Bitcoin-asset or currency? Revealing users hidden intentions.

Hernandez- Castro, J. Darren Hurley-Smith. (2017). *Altcoins: Alternative to bitcoin and their increasing presence in malware-related cybercrime.*

Jeimi. J. (2017). *Blockchain: Cadena de bloques. Reflexiones sobre seguridad y control*. En *Revista SISTEMAS*.

Parrondo, L. (2008). *Tecnología blockchain, una nueva era para la empresa"* En *Revista de Contabilidad y Dirección.* Vol. 27.

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet.* Barcelona, 2017.

Uría Menéndez. (2018). *Tecnología Blockchain: Funcionamiento, Aplicaciones y Retos Jurídicos Relacionados.* En *Actualidad Jurídica Uría Menéndez*.

7. WEBGRAFÍA

Barceló Ferre, Iris. (2021). Criptomoneda: Qué es, definición y concepto. *Economipedia*. Recuperado de https://economipedia.com/definiciones/criptomoneda.html

Bernal Johans. (2018). Historia de las Criptomonedas. *Criptoleaks*. Recuperado de https://criptoleaks.com/la-historia-de-las-criptomonedas/

Bitcoin: Origen, funcionalidades y riesgos de la moneda virtual (2010). En Finanzas para todos. Recuperado de https://www.finanzasparatodos.es/es/secciones/actualidad/bitcoin.html

Borman, D. (2020). Guía definitiva para el halving de Bitcoin de 2020. *Beincrypto*. Recuperado de https://es.beincrypto.com/aprende/guia-definitiva-halving-bitcoin-btc-2020/

Cómo elegir una cartera de Bitcoin y otras criptomonedas. *(2020). En* Criptonoticias. Recuperado de https://www.criptonoticias.com/criptopedia/como-elegir-monedero-cartera-bitcoin-criptomonedas-criptoactivos/

Divisas. El Mercado de Divisas. En Asturias Corporación Universitaria. Recuperado de https://www.centro-virtual.com/recursos/biblioteca/pdf/mercado_divisas/unidad2_pdf1.pdf

El origen de Bitcoin y Blockchain, ¿inventados desde cero por un desconocido? (2019) En Santander Global Tech. Recuperado de https://santanderglobaltech.com/origen-bitcoin-blockchain-inventados-desde-cero-por-un-desconocido/

Ferruz, Luis. (2017). La burbuja de las criptomonedas: el caso del bitcoin. *Expansión*. Recuperado de https://www.expansion.com/opinion/2017/11/17/5a0f0f8b22601d1c268b45a9.html

Historia de las Criptomonedas. (2019). En Instituto Nacional de Ciberseguridad. Recuperado de https://www.osi.es/es/campanas/criptomonedas/historia-criptomonedas

Maldonado, J. (2020) Nueva Ley Española para establecer un control estricto sobre las criptomonedas. *Bit2news*. Recuperado de www.news.bit2me.com

Oliva, Ricardo. (2021) Regulación legal del Bitcoin y de otras criptomonedas en España. En *Algoritmolegal*. Recuperado de https://www.algoritmolegal.com/tecnologias-disruptivas/regulacion-legal-del-bitcoin-y-de-otras-criptomonedas-en-espana/

Pastorino, Cecilia. (2018). Blockchain: qué es, cómo funciona y cómo se está usando en el mercado. Recuperado de https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

Pérez, Xesús. (2017). Las Criptomonedas: Consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España En Revista de Derecho Penal y Criminología. Recuperado de http://revistas.uned.es/index.php/RDPC/article/viewFile/24454/19303

Qué es Bitcoin (BTC) (2020). En Criptonoticias. Recuperado de https://www.criptonoticias.com/criptopedia/que-es-bitcoin-btc/

¿Qué son las ICO de criptomonedas? (2021). En *Bit2meAcademy.* Recuperado de https://academy.bit2me.com/ico-criptomonedas/

¿Qué es una wallet o monedero de criptomonedas? *(2020).* En *Bit2meAcademy*. Recuperado de https://academy.bit2me.com/wallet-monederos-criptomonedas/

¿Qué es LiteCoin? (2021). En *LiteCoin.* Recuperado de https://litecoin.org/es/

¿Qué es una blockchain y para qué se utiliza? (2018). En *Holded*. Recuperado de https://www.holded.com/es/blog/una-blockchain-se-utiliza

Sánchez, Julia. (2018). Criptomonedas. Recuperado de https://www.pj.gov.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf

Zhu, Y. (2017) Qué es y cómo nació el Bitcoin. *Rankia*. Recuperado de https://www.rankia.com/blog/blockchain-criptomonedas-bitcoin-ethereum/3669482-que-como-nacio-bitcoin