Quaderns IAFI. Revista científica grup de recerca IAFI
Volum 1. Pàgines 127 a 158

BITCOIN: ¿LA MONEDA DEL FUTURO?

ADRIÀ MARTIN
MARIA ÀNGELS PONS
Departament de Matemàtica Econòmica, Financera i Actuarial
Universitat de Barcelona
Avda. Diagonal 690, 08034 - Barcelona

RESUMEN:
En el artículo que encontrareis a continuación veremos como Bitcoin, y las criptomonedas en general, son una alternativa muy a tener en cuenta al dinero corriente actual. Aunque este sistema aún está en un proceso experimental, propone unas ideas y posibilidades de uso muy revolucionarias, además de presentar una serie de ventajas respecto al dinero corriente que lo posicionan como el sustituto natural a este. El Bitcoin no es ni bueno ni malo en sí mismo, sino que, si es una cosa o la otra dependerá directamente del uso que hagamos de él, al igual que el dinero. Bitcoin, y el resto de las criptomonedas que encontramos en el mercado, sientan sus bases sobre la tecnología Blockchain, un sistema revolucionario y mucho más eficiente de la gestión de la información, además, su aplicación no se restringe únicamente al sector financiero, sino que, sus usos van más allá de este y es extrapolable a otros ámbitos.

PALABRAS CLAVE: Bitcoin, Etherum, Satoshi Nakamoto, bloque génesis, criptomoneda o criptodivisa, brainwallet, pools de minería, criptografía de clave pública, “blockchain” o cadena de bloques, monederos digitales
CÓDIGOS JEL: E40, E50

BITCOIN: THE CURRENCY OF FUTURE?

Bitcoin is the trendiest cryptocurrency nowadays by the incredible growth of value that has been. Recently many people has been interested in that crypto currency seen her growing popularity and globalization. The crypto currencies and block chain technology, they are something completely new for the transactions and payments system and the world in general since it changes completely the current financial system.
First of all, a crypto currency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. It works the same way as current money, with the difference that doesn’t exist in physical form, but it is in the network, in bits. Recently, the value of the cryptocurrencies, and especially Bitcoin, has fluctuated a lot in the exchange market caused by different reasons, but the most important is the speculation. Seeing that, the investors have reported the problem associated with this and the bubble that is creating and feeding this practice.
Blockchain, the technology behind Bitcoin and the others cryptocurrencies, offers very good ideas and with various non-economic applications that improve many aspects of our lives that, with the current model we won’t get.

They represent a revolutionary and radical change on our conception of the economy and global finance, as well as proposing a kind of ideas and applications much better and more efficient that we use nowadays.
Bitcoin, and the rest of cryptocurrencies, as well, of course, the Blockchain technology, represent a complete break with the current centralized information management such as finance model also it's more efficient and secure way to manage our information.

KEY WORDS: Bitcoin, Etherum, Satoshi Nakamoto, block genesis, cryptocurrencies, brain wallets, mining pools, public key cryptography, Blockchain technology, digital wallets
JEL CODES: E40, E50

BITCOIN: ¿LA MONEDA DEL FUTURO?

1. INTRODUCCIÓN:

En este trabajo he querido realizar un estudio sobre, qué es el Bitcoin, en qué se basa, sus ventajas e inconvenientes, sus diferencias respecto a la moneda tradicional y, si es posible que esta criptomoneda, el Bitcoin, sustituya completamente, o por lo menos, que se generalice su uso, a la moneda de curso legal que usamos hoy en día para cualquier transacción que realicemos y qué consecuencias traería.

Bitcoin, al igual que cualquier cosa en este mundo, cuenta con sus defensores y con sus detractores, al grupo al que se quiera pertenecer ya depende del criterio de cada uno y de su ideología y conocimientos de la economía, aunque nadie podrá dudar ni negar que, las criptomonedas están pisando fuerte y han logrado provocar que muchas instituciones, tanto entidades bancarias como Estados al completo, se las considere muy seriamente como un competidor potencial y hayan puesto su foco de atención en ellas, ganándose así el respeto de muchos, puesto que han logrado hacerse un hueco en la economía mundial y hacer temblar el oligopolio financiero que lleva reinando en el mundo estas últimas décadas.

El mundo de las criptomonedas es algo complejo y volátil, aunque, si nos quedamos únicamente con la idea, vemos que propone algo totalmente innovador y diferente en un sector donde los cambios no son bienvenidos y los usuarios son reticentes a estos. Aunque, desde el punto de vista del usuario, los servicios y características que presentan esta nueva forma de dinero, es un sistema mucho más eficiente, rápido, seguro, y otorga a los usuarios un poder y control sobre sus finanzas nunca antes visto.

Las criptomonedas, toda y la gran cantidad de ventajas que presentan y mejoras respecto al dinero fiduciario, todavía necesitan tiempo para adquirir la experiencia necesaria para sustituir por completo al dinero, puesto que, dado que son de muy reciente creación, todavía se encuentran en una etapa muy experimental de

aprendizaje y de analizar y darse cuenta de las flaquezas y debilidades que tienen, y eso sólo se adquiere mediante el tiempo. Aunque proponen una serie de ideas muy revolucionarias y originales, no pueden competir, en cuanto a experiencia se refiere, con el dinero fiduciario, el cual su origen se remonta al siglo V a.C. y que continuamos utilizando hoy en día, con los cambios que ha ido sufriendo a lo largo de su historia.

Dentro de este mundo, el de las criptomonedas, tan diverso, pese a que Bitcoin es la primera que se nos viene a la mente cuando oímos hablar de monedas digitales, existen cientos de alternativas a esta, algunas de ellas presentan características que las hacen mejores que su primogénita. Por lo que, si se quiere invertir en criptomonedas o adquirirlas para utilizarlas como medio de pago y cambio para nuestras transacciones no es menester tener que comprar Bitcoin para ello (y menos mal, porque últimamente está adquiriendo unos valores que escapan a la mayoría de los bolsillos) sino que podemos optar por alguna de sus alternativas, las cuales son bastante más baratas y eso no quiere decir que tengan que ser peores, ya que muchas de estas superan en funcionalidad a Bitcoin, puesto que fueron creadas para solventar los problemas y mejorar sus capacidades y servicios.

Por lo tanto, no es algo binario, o Bitcoin o nada, sino que existe todo un abanico de posibilidades iguales, o mejores, a este.

II. LAS CRIPTODIVISAS Y EL BITCOIN

2.1 ¿Qué es una criptomoneda?

Una criptomoneda, o criptodivisa, no es más que un medio de intercambio, al igual que el dinero corriente, con el que podemos adquirir cualquier tipo de bien o servicio, con la diferencia de que esta primera no es física, no es tangible, sino que se trata de una moneda digital, la cual, mediante la Blockchain, la cual funciona como un gran libro contable donde se registran todas las transacciones realizadas por cualquier criptomoneda.

Así, para que pueda considerarse una moneda digital y por lo tanto, cumplir con su misión como medio de intercambio de bienes y servicios tiene que reunir una serie

de cualidades, las cuales se denominan las cualidades del buen dinero y son las siguientes:

- **Depósito de valor:** Que sea capaz de atesorar y acumular valor con el paso del tiempo. Si perdiera valor con el tiempo, no sería rentable mantenerla y por lo tanto, con el tiempo desaparecería.

- **Unidad de cuenta:** Que permita la fijación del precio de los bienes y servicios que pretende adquirir.

- **Medio de cambio:** Como toda moneda corriente y uno de sus principales usos, tiene que ser capaz de poder adquirir bienes y servicios a cambio de ella.

- **Invariancia física:** Tiene que asegurar que sus propiedades físicas no cambian a lo largo del tiempo.

- **Homogeneidad:** Tiene que haber una igualdad en la naturaleza o género, es decir, tienen que ser idéntica entre ellas.

- **Bajo ratio flow / stock.**

- **Empleabilidad:** Su tamaño debe ser práctico, de fácil transporte y llevable.

- **Accesibilidad:** Que sea alcanzable por un gran número de personas para que sean capaces de utilizarla. Por lo tanto, si una moneda, sea digital o física, cumple estas condiciones, se ha ganado el derecho a que se la pueda considerar una “buena” moneda. Las criptomonedas cumplen esta serie de condiciones, por lo que parece razonable que se postule como una buena alternativa al dinero corriente, dado que, por mucho que consideremos a este “buen dinero” no cumple con todas las condiciones que se le piden a una moneda para poder considerarla dinero. Por lo que se nos plantea la siguiente cuestión: ¿No se está convirtiendo el dinero de curso legal en un mero medio de intercambio? Porque, por ejemplo, si analizamos la primera condición que debería reunir, la de depósito de valor, comprobamos que, dada la existencia de la inflación, no es posible saber qué voy a poder adquirir con una cantidad

X de cualquier moneda que conocemos (pongamos el dólar) el próximo año, no parece ser un depósito de valor muy fiable.

Si tuviéramos que dar una definición de dinero, ya estemos hablando de dinero corriente o digital, sería algo parecido a: “cualquier cosa que los miembros de una comunidad están dispuestos a aceptar como pago de bienes o de deudas dentro de una economía”. Citación de Santiago Márquez Solís (2016) en su manual, Bitcoin: guía completa de la moneda del futuro.

Y así, hemos llegado a otro concepto importante, **economía.** Esta no es ni más ni menos que, la manera en la que los usuarios interactúan entre ellos para obtener el máximo beneficio posible dados unos recursos limitados. Al ser estos limitados, tenemos que administrarlos del modo más eficaz y eficiente posible para alcanzar el fin último, la maximización del beneficio personal.

2.2 ¿Por qué existen tantas criptomonedas diferentes?

Aunque actualmente sólo unas pocas monedas digitales son conocidas, como Bitcoin, Litecoin, Dogecoin, Coinbase, a día de hoy existen unas 700 criptomonedas diferentes, todas surgidas a partir del Bitcoin, la pionera en este sector. El valor de la gran mayoría de éstas es cero o muy próximo a él, por lo tanto, sería poco elegante tenerlas en cuenta.

Existen dos motivos principales por los que en esta última década han surgido tantísimas monedas digitales, el primero sería la oportunidad de adopción, y la segunda, la oportunidad de mejora.

- **Oportunidad de adopción:** Cuando “nace” una nueva moneda, los primeros usuarios en adoptarla y utilizarla son los que tiene una mayor probabilidad de ganar dinero si esta llega a popularizarse y extenderse su uso. Dado que al inicio de la creación de una moneda, su valor es ínfimo, es fácil adquirir un gran número de ésta por un valor mínimo, con el objetivo y la confianza que con el transcurso del tiempo, esta moneda se popularice y por lo tanto, que su valor aumente junto con su demanda. Cuando uno de estos primeros usuarios, que la adquirió por un valor muy inferior al que ha alcanzado en

dicho momento, considere oportuno, oferte la cantidad de moneda que posee a un precio mucho más elevado de lo que le costó en su momento, y ganar así grandes cantidades de dinero sin apenas esfuerzo, únicamente con visión de futuro. Esto es a lo que comúnmente se denomina especulación.

- **Oportunidad de mejora:** Como la mayoría de las nuevas criptomonedas que se crean hoy en día se derivan del Bitcoin, es razonable que, se analicen las debilidades y errores de ésta, y se intenten subsanar, postulándose como una mejor alternativa que su predecesor.

Algunas de estas mejoras podrían ser la de reducir el tiempo que una transacción tarda en ser confirmada. Una transacción de Bitcoin tarda unos 10 minutos, mientras que una de Litecoin (una alternativa al Bitcoin y creada precisamente para solventar las carencias de ésta), se demora alrededor de unos 2,5 minutos, y en el caso del Dogecoin, consigue acortar esta espera a 1 minuto.

¿Tienen sentido todas estas alternativas a Bitcoin?

Después de ver que existen cientos de criptomonedas distintas a Bitcoin, se nos plantea una cuestión importante para entender porque Bitcoin es la mejor y más popular entre sus alternativas. Esta cuestión es la siguiente: ¿Tienen sentido, entonces, la existencia de tantas criptomonedas diferentes a Bitcoin? Intentaré dar una respuesta lo más razonada posible.

Dada la popularidad que ha tenido Bitcoin desde su creación, no es raro la aparición de cientos de imitaciones a ésta, muchas de las cuales siguen un algoritmo o esquema idéntico o muy parecido, creándose incluso a partir del mismo código fuente que su precursora, o como otras, empezando desde cero, con codificaciones totalmente distintas a Bitcoin.

La popularización y conocimiento de Bitcoin, en parte ha estado gracias a los medios de comunicación, tan extendidos e influyentes en la actualidad. Si se hubiera creado hace unos 20 años, probablemente no habría tenido apenas repercusión como la ha tenido a día de hoy.

Las alternativas de Bitcoin adoptan, por tanto, un papel mucho más secundario, además de aportar otra panorámica y punto de vista que, Bitcoin aprovecha para mejorar y corregir los posibles errores que puedan existir en su software, por lo tanto, éstas contribuyen, valga la redundancia, a fortalecer (y no a debilitar, objetivo por lo que son creadas) a Bitcoin, con esto no quiero decir que estas alternativas sean malas o inútiles, sino que, Bitcoin las utiliza para "retroalimentarse" y darse cuenta de sus debilidades.

Entonces, ¿todas estas criptomonedas derivadas de Bitcoin no sirven para nada o es que, su futuro cercano sería su propia desaparición? En absoluto, a pesar de que dudo que en un futuro Bitcoin sea superado por alguna de estas *altcoins* eso no quiere decir que éstas no tengan su hueco en el ciberespacio. Dado que vivimos en un mundo cada vez más globalizado e interconectado, es buena la existencia de estas altcoins para facilitar las interacciones entre miembros de una misma comunidad, al igual que las distintas divisas que existen en el mundo. Y, de entre todas ellas, como si de una pirámide se tratase, en la cúspide tendríamos a la más popular, líquida y aceptada de entre ellas, Bitcoin.

Una vez argumentado el porqué de la existencia de las distintas alternativas a Bitcoin, nos surge otro término, de importante explicación, para entender de una manera más amplia y profunda todo este mundo de las criptomonedas. El término al que hago referencia es, **la liquidez,** que explica la capacidad de convertir una cosa en otra. Para ello tiene que reunir y respetar tres propiedades:

- **Rapidez:** Que dicho intercambio se produzca en tiempo real, al momento, o en su defecto, en el menor tiempo posible.

- **Pérdida de valor:** Que mantenga a lo largo del tiempo su valor, que ni lo pierda ni lo gane, que no sufra fluctuaciones (aunque esto, dado el mundo en constante cambio en el que vivimos, es algo imposible de cumplir).

- **Temporalidad:** Que dicho intercambio se produzca cuando yo considere oportuno, que nada me impida hacerlo cuando yo quiera.

La liquidez actúa como “escudo” frente a la incertidumbre, ante imprevistos, dado que, si yo poseo algo muy líquido, sabré que, en cualquier momento, podré cambiarlo por cualquier cosa, y, ante cualquier contratiempo estaré relativamente protegido frente a algo de una liquidez muy baja.

Bitcoin es la criptomoneda más líquida que existe a día de hoy, dado que, es la que mayores facilidades de intercambio presenta, es la que con mayor facilidad podemos cambiar por otra cosa, incluidas otras criptomonedas.

Bitcoin en la actualidad

Desde mediados del año 2017, Bitcoin ha ido adquiriendo una popularidad creciente a cada día que pasaba y acaparando las portadas de infinidad de periódicos, paginas y blogs de actualidad. Si nos remontamos al año 2016, Bitcoin era meramente un activo más del mercado, en el cual únicamente algunos inversores invertían dinero y, sólo un grupo reducido de personas lo utilizaban con su principal finalidad, la de adquirir cualquier bien o servicio que se quiera.

La fama de Bitcoin es muy reciente, concretamente desde finales de marzo del 2.017, cuando Bitcoin logró romper la barrera de los 1.000 dólares, hito nunca antes conseguido. A partir de ese momento, esta criptomoneda tomó una tendencia creciente imparable y descomunal. Este crecimiento se ha visto mermado en diversas ocasiones, aunque durante breves periodos de tiempo y, una vez superado el bache, retomó su senda de crecimiento desmesurado. Esta tendencia alcista es tal que, a día de hoy, Bitcoin cotiza a nada más y nada menos que 16.000 dólares, algo más de un 4.000% respecto a su valor en sus inicios por allá 2013, y es que, tan solo en 2017, Bitcoin ha subido un 649%.

Bitcoin sigue rompiendo records como si nada y por ahora, su crecimiento parece no tener techo. Estas variaciones tan abruptas y sin seguir ningún patrón le ha servido a sus detractores para criticarlo y desacreditarlo utilizando argumentos como que, se trata de otra burbuja más que tarde o temprano explotará. Siendo objetivos, sí que parece estar adoptando un crecimiento demasiado acelerado y alcanzando cotizaciones históricas. Además, recientemente, Bitcoin ha sufrido un hackeo masivo

en Youbit, una de las mayores plataformas Bitcoin del mercado surcoreano que hizo que su valor se desplomará hasta un 15%. A raíz de este ciberataque, la plataforma se vio obligada a declararse en bancarrota, permitiendo únicamente recuperar el 75% de los fondos que los clientes tenían depositados en sus monederos digitales dando el resto por perdido e irrecuperable. Este desplome vino justo después de que Bitcoin tocará techo cotizándose a 20.000 dólares. Con este suceso, el valor de mercado de la criptomoneda cayó hasta los 11.000 dólares, casi un 30%, aunque, como he comentado unas líneas más arriba, esta caída se ha visto compensada esta semana (a 26/12/2017) con una subida en tan sólo un día del 10% y alcanzando de nuevo los 15.000 dólares.

Con un precio tan fluctuante, las autoridades y personajes públicos de renombre han salido al paso y aprovechando para “meter más el dedo en la llaga”, y criticarlo y hundirlo más, argumentando que estos aumentos es su precio vienen impulsados y generados por la especulación y que, tarde o temprano, se producirá una fuerte caída de su precio, haciendo explotar la burbuja que está creando.

Dada la popularidad creciente que atesora Bitcoin, nacieron a partir de él diversas criptomonedas, algunas de ellas creadas como sátira y critica a esta y al dinero virtual en general. Una de las más famosas y la que, en los últimos meses, potenciada en parte por la burbuja que está generando el crecimiento desmesurado del precio de Bitcoin, ha experimentado un crecimiento más significativo, estoy hablando de Dogecoin. Un criptomoneda creada en 2013 como crítica a la seriedad con la que muchos se toman Bitcoin. En común, estas dos monedas virtuales, únicamente tenían tecnologías y códigos parecidos, pero nada más, ya que el fin de Dogecoin no era otro que el de burlarse de Bitcoin. La burla se extendía desde la imagen identificativa de esta criptomoneda hasta su propio nombre (basado en la raza de perro japonesa Shiba Inu, también conocida como “doge”).

Billy Markus, creador de esta cómica moneda no le atribuyo ningún valor a su creación ya que no espera utilizarla para nada más que para mofarse de Bitcoin. Pero, como el valor de las monedas virtuales lo fija el mercado y no ningún individuo o entidad, su precio, en 2014, se triplicó en pocas horas hasta alcanzar los 0,018 dólares, provocado por un cambio legislativo que se produjo en China, la cual ponía

restricciones y nuevas trabas a la inversión en Bitcoin. Este crecimiento fue meramente anecdótico, ya que poco después su valor cayó hasta los 0,0002 dólares y, este se mantuvo durante los dos años siguientes.

Pero, en 2017, Bitcoin empezó a experimentar su mayor crecimiento desde su creación, llegando a multiplicar su precio por 10, lo que provocó que otras criptomonedas más baratas también incrementaran su precio, Dogecoin alcanzó los 0,0004 dólares, aunque, no fue hasta enero de 2018 que el precio de Dogecoin se multiplicó por 7 sin ninguna razón aparente, llegando incluso a preocupar a su propio creador, el cual declaró : ”*creo que dice mucho del espacio de las criptomonedas que una moneda con un perro dibujado que no ha sido actualizada en más de dos años supere los mil millones de valoración*”.

A día de hoy se han generado un total de casi 113 mil millones de Dogecoin, que al superar la barrera del centavo de dólar por unidad sorprendía a todos y superaba los mil millones. Este repentino ascenso ha atraído a otros inversores que procedieron a doblar el precio con la finalidad de poder especular con esta moneda y venderla por un precio muy superior al que la compraron. Pero Dogecoin ejemplifica muy bien en 2018 los problemas de las monedas virtuales y la finalidad principal de esta criptomoneda, que no es otra que la de poner en evidencia la inestabilidad e insolvencia de las monedas virtuales que tan de moda se están poniendo en estos días.

Dogecoin refleja muy fiel y claramente los excesos de los inversores en criptomonedas y la burbuja que están generando con ello, con el único fin de especular como si de un activo financiero tratara y llegar a ganar grandes cantidades de dinero. Con esta criptomoneda podemos apreciar como el mercado de las criptomonedas se está descontrolando y volviendo loco, abandonando su finalidad principal y adoptando otra nueva, como nuevo activo de especulación para los inversores.

III. EL BITCOIN Y SUS APLICACIONES

Bitcoin es una moneda creada en 2009 por Satoshi Nakamoto. Como cualquier otra divisa que exista hoy en día en cualquier economía del mundo, con ella podemos adquirir bienes y servicios, utilizarla como depósito de valor, con la diferencia de que esta, Bitcoin, es una divisa electrónica, completamente descentralizada, lo que la hace más eficiente y estable frente a otra divisa controlada por algún Gobierno o Estado. Esta criptomoneda, una de las muchas que existen actualmente como Litecoin, Dogecoin, Namecoin..., pero, por muchas de sus características, la más importante y utilizada de ellas, difiere de la moneda corriente en que no precisa de intermediarios, es decir, se transfiere de persona a persona directamente, sin necesidad de ningún banco o terceros.

A partir del Bitcoin, han surgido cientos de monedas electrónicas. A día de hoy, existen 667 monedas virtuales, y este número crece a diario, aunque la gran mayoría de estas criptomonedas, tienen un valor nulo o muy cercano a cero, por lo que no tienen relevancia en el mercado actual de las monedas virtuales.

Una vez hecha esta pequeña introducción y esta breve explicación sobre sus orígenes, me gustaría analizar por qué en este último año Bitcoin ha ganado tanto protagonismo, llegando incluso a romper un récord histórico al trepar hasta casi los 12.000 dólares en la bolsa. Para ello, expondré una serie de ventajas que posee Bitcoin y que se posicionan como una mejor opción que el dinero fiduciario que utilizamos hoy en día. Algunas de estas ventajas son las siguientes:

1. Rápido: Cualquier envío que se realice de Bitcoines, sea cual sea la cantidad y su destino, se demora tan sólo unos minutos, a diferencia que realizar una transferencia con dinero corriente, que puede llegar a retrasarse hasta días.

2. Barato: Al realizar una transferencia a cualquier parte del mundo desde tu propio banco puedes tener unos costes desmesurados, mientras que, si esa misma transferencia se hace a través de Bitcoines, el coste de ésta se reduce a unos meros céntimos o incluso llegando a ser gratuita.

3. Global: Puedes enviar Bitcoines a cualquier parte y país del mundo, sin entender

de fronteras ni restricciones.

4. Descentralizado: Bitcoin no está, ni puede ser controlado por ningún gobierno ni banco central existente, por lo tanto, no pueden decidir ni intervenir en su precio, ni su creación. Se trata de una moneda totalmente despolitizada, es la misma comunidad la que ejerce un control sobre ella.

5. Propio de cada usuario: El mismo usuario de la cuenta de Bitcoin es el único propietario de ellos, al 100%, sin posibilidades de ser intervenida ni bloquear su cuenta. Uno mismo es su propio "banco".

6. Seguridad y distribución: Bitcoin es muy seguro, incluso mucho más que el dinero fiduciario. Esto es gracias a que su código está protegido por una de las criptografías más potentes que existen actualmente, más incluso que el que se usa en los bancos. Incluso ante una tormenta solar Bitcoin, al contrario de otros sistemas, resistiría. Esto es debido a que algunos de sus nodos se encuentran en bunkers de la segunda guerra mundial, protegidos bajo tierra e incluso triple seguridad perimetral.

7. Transparente: Todas las transacciones que se realizan con Bitcoines quedan registradas en la Blockchain, siendo esta totalmente pública.

8. Emisión limitada: Su creación está restringida a 21 millones de Bitcoines, por lo tanto, nadie puede generar miles de Bitcoines de la noche a la mañana. Su minación, sigue una serie de reglas que son aprobadas por la comunidad, la democracia es la que realmente controla Bitcoin.

9. Sin costes adicionales: Abrirse una billetera o monedero digital es totalmente gratuito y en ella puedes almacenar tantos Bitcoines como quieras. Además, se pueden realizar transferencia allí donde uno quiera sin apenas costes (frente a los costes que sí que tendría una transferencia realizada desde un banco). A parte del desembolso por la compra de Bitcoines, no existen más costes añadidos, ni cobros por suscripción, mantenimiento, etc.

10. Anonimidad: Bitcoin no es completamente anónimo, pero trabaja para serlo.

Estas características inherentes a todas las criptomonedas, algunas las cumplen en mayor medida que otras, les otorgan un plus y una posición ventajosa respecto el dinero fiduciario de hoy en día y una mejor alternativa en las transacciones y pagos que se realizan globalmente hoy en día puesto que el dinero que utilizamos actualmente no cumple ni la mitad de las características que acabamos de enumerar y otorgar a las critpodivisas.

Su creación es relativamente sencilla para todo aquel que tenga unos conocimientos básicos de informática y de creación de algoritmos. Todo empieza con la descarga de un programa concreto, el cual registra y verifica todas las transacciones de Bitcoines que se realizan, que cualquiera puede descargar de Internet, dado que es totalmente público, al igual que su código. Los usuarios que descargan y generan Bitcoines son conocidos como “mineros”.

A través de diversos procesos, el minero es recompensado con esta moneda. A medida que los “mineros” van trabajando, se crean nuevos Bitcoines y se introducen en el mercado, pero este proceso no puede ser infinito, y minar millones de Bitcoines, sino que se ha fijado un límite a la cantidad de Bitcoines que hay en el mercado, concretamente se ha limitado a 21 millones, una vez alcanzada dicha cifra, nadie puede seguir minando Bitcoines e introducirlos en el mercado, por lo que no se concibe la posibilidad de una inflación por exceso de Bitcoines en el mercado. Este sistema, dado que está formado por ordenadores de todo el mundo, es un sistema totalmente descentralizado que ninguna entidad puede controlar, es la propia comunidad la que acuerda las reglas que regulan Bitcoin.

Después de entender de dónde provienen los Bitcoines, se nos plantea una nueva duda sobre esta criptomoneda, entonces, si no depende de ningún Estado ni banco, ¿dónde se fija el precio de Bitcoin?

El precio de Bitcoin, como si de un valor bursátil se tratara, depende de la oferta y la demanda que exista en el momento de comprarlo o venderlo. Por lo tanto, es directamente proporcional, así cuando la demanda de este aumente, también lo hará su precio y viceversa. Por tanto, su precio depende directamente del mercado y nunca de bancos centrales ni instituciones. Desde su creación, por allá 2009, su

precio ha aumentado exponencialmente, llegando a cotizar, a fecha de 5 de diciembre de 2017, momento en el cual redacto este trabajo, 12.130 dólares, unos 10.250 euros.

En el gráfico que adjunto a continuación, en el gráfico no4, se puede apreciar muy claramente el gran aumento de su precio desde diciembre de 2016, cuando apenas llegaba a 1.000 dólares hasta alcanzar los 12.000 dólares anteriormente citados.

Para concluir con este apartado sobre Bitcoin, y antes de entrar a analizar sus usos más frecuentes y extendidos de Bitcoin, me gustaría hacer referencia a una frase sobre esta famosa criptomoneda que se publicó, en enero de 2015 en el prestigioso diario americano *Wall Street Journal*, en la que hablaba sobre el potencial de esta, la frase era la siguiente:

"Bitcoin es radicalmente nuevo, un sistema descentralizado de la manera que la sociedad gestiona el intercambio de valor. Es, sencillamente, una de las innovaciones más potentes en las finanzas de los últimos 500 años"

Por lo tanto, si un medio de comunicación tan importante e influyente como es éste dice lo anterior, algo de razón debe de llevar.

La finalidad principal de la existencia de una moneda, y la que determinará su valor (y la duración de su existencia) es su uso para "algo", las utilidades que le podemos dar a una divisa, es decir, el abanico de posibilidades que me oferta una moneda, en este caso, los usos que le podemos dar a Bitcoin.

2.3 El pago por Internet

Dado que hoy en día, muchas de las transacciones que se producen en una economía se realizan a través de la red, sería impensable, e ilógico, que una moneda, precisamente creada y únicamente existente en la red dado que no existen de manera física como el dinero corriente que entre sus usos no estuviera

precisamente su utilización en internet. Éste es su uso más corriente y extendido. Si Bitcoin es una criptomoneda, ¿habrá algún sitio donde la podré intercambiar por algo de mi interés? Entonces, ¿qué se puede adquirir con Bitcoines?

Prácticamente lo que el usuario quiera, dada la creciente popularización de las criptomonedas, y en especial del Bitcoin, actualmente y a cada momento más, hay infinidad de portales y sitios donde ya se aceptan Bitcoines, y por lo tanto, criptomonedas, para el pago de cualquier compra que se realice, ya sean viajes, todo tipo de artículos, e incluso el pago de una nómina por parte de algunas empresas a sus trabajadores!

Según la guía completa de la moneda del futuro: "*El inicio de las compras con Bitcoin es curioso y poco común. Nos remontamos a mayo de 2010, en concreto el día 22, cuando un programador de Florida llamado Laszlo Hanyecz y activo miembro del foro BitcoinTalk, anunció en este que pagaría 10.000 Bitcoines a quien le comprara dos pizzas. El reto quedó lanzado en la Red y sería otro programador, pero en este caso del Reino Unido, quien aceptó dicho reto y ni corto ni perezoso compró telefónicamente un par de pizzas de pepperoni en Papa John's de Jacksonville con su tarjeta de crédito, y pidió que las entregaran en el domicilio de Laszlo, quien posteriormente pagó los 10.000 Bitcoines prometidos".*

A día de hoy la lista de establecimientos, no sólo virtuales, sino también físicos que aceptan el pago de sus productos o servicios con Bitcoin es larguísima y más extensa a cada momento que pasa.

2.4 Otros usos

Otro de los usos que se le puede dar a Bitcoin, y a cualquier criptomoneda en general, es el de su utilización como moneda refugio. Como las monedas digitales no dependen de ningún Estado ni organismo supranacional, si se diera una situación de crisis o algún suceso que golpeará la economía que provocara una caída drástica del precio y valor de la moneda de dicho país/estado afectado, las criptomonedas podrían servir como refugio o "caja fuerte" de nuestros fondos, sin miedo a que algún

suceso externo pueda provocar que lo perdamos todo. Cuando uno de estos hechos sucede, la gente tiende a refugiar su dinero en inversiones independientes, como el oro o el Bitcoin, valores “seguros” que nos garantizan que no perderán valor ante cualquier hecho económico.

2.5 Moneda utilizada por los ciberdelincuentes

Hoy en día, como se ha demostrado en los últimos ciberataques, Bitcoin es un medio de pago ideal para pedir un rescate o soborno. Dada su naturaleza, las criptomonedas dificultan la identificación del origen o procedencia de los delincuentes que la utilizan para financiar sus fechorías.

Aunque la mayoría de personas utilizan la moneda digital para fines legales, como pueden ser la inversión o su utilización para adquirir bienes o servicios sin quebrantar la ley, los últimos ciberataques y la utilización de las criptomonedas por parte de estos ciberdelincuentes para fines ilícitos han causado que la imagen de las criptomonedas se vea ensuciada y asociadas al uso criminal y no para el que fueron creadas, su uso legal como medio de cambio o adquisición de bienes.

La criptografía, su sistema de seguridad, de la moneda garantiza su anonimato en un primer momento. Ladificultad de rastrear la criptomonedaha sido la razón por la que los ciberdelincuentes se han decantado por elegir las criptomonedas como su dinero criminal.

Otra de las razones que han impulsado su uso dentro del mundo criminal para fines delictivos se fundamenta en motivos puramente económicos, como podría ser el blanqueo de capitales obtenidos por medios ilegales.

Una vez analizado, qué es una criptomoneda, qué es Bitcoin, como se fija su valor, sus usos y ventajas frente al dinero fiduciario, voy a entrar a hablar de otro concepto muy importante dentro del mundo de las monedas digitales, este concepto es el de los monederos o billeteras digitales.

Y, es que, un monedero o billetera digital no dista mucho de su homónimo físico,

este, no es ni más ni menos que un lugar donde almacenar, guardar y transportar tus criptomonedas, pero, en este caso, dentro de la red, al igual que harías con tu billetera física, en la cual guardas tus billetes y/o monedas de la moneda que utilices asiduamente.

Empecemos por el principio, para poder empezar a operar con cualquier criptomoneda, es menester de disponer de una aplicación, la cual debes descargar de la red, e instalarla y configurarla en tu ordenador o dispositivo móvil, que no hace otra función que la de almacenar tus criptomonedas.

Todos estos monederos digitales cuentan con altos niveles de seguridad para proteger tu dinero digital de posibles ciberataques, esta sistema de seguridad se denomina criptografía (concepto en el que profundizaré unos capítulos más adelante en este trabajo) y funciona de la siguiente manera, el usuario asigna una contraseña o clave secreta a las direcciones que tenemos asociadas a nuestra billetera digital, pero, como eso no es suficiente para asegurar nuestro dinero, se añade otra clave adicional para poder acceder a nuestro monedero digital, elevando el grado de seguridad frente a cualquiera, distinto al propietario de dicha billetera, que quiera entrar en ella.

IV. LA CREACIÓN Y OBTENCIÓN DE BITCONES

En este capítulo analizaremos las diferentes opciones que tenemos para obtener Bitcoines. Para simplificar un poco todo este proceso, que suele ser la parte más complicada para aquel usuario que quiere poseer Bitcoines, analizaremos dos de los métodos más popularizados para generar esta criptomoneda. Estos son:

1. Los métodos tradicionales: Éste proceso podríamos asignarle el título de proceso pionero en la creación y obtención de Bitcoines. Dentro de estos métodos encontraríamos el famoso método de “minar una criptomoneda”, el método de los grifos...

2. Los “otros” métodos: Se refiere a cualquiera de los métodos que se utilicen para

obtener Bitcoines diferente a los métodos tradicionales.

4.1. Los métodos tradicionales

4.1.1 El proceso de la minería

Fue el primer método que se utilizó para crear una criptomoneda. Minar por tanto, una moneda consiste en, el minero, que es el usuario que utiliza este procesa para obtener una criptomoneda, debe encontrar una solución al problema computacional que el algoritmo que esté utilizando para minar dicha moneda le plantee. En los inicios de Bitcoin, la minería era un proceso relativamente sencillo para aquellos con un conocimiento básico de algoritmos, dado que únicamente requería un ordenador y poner en práctica dichos conocimientos. Pero, cuando las criptomonedas empezaron a popularizarse, el proceso se empezó a volver más complejo, y ya no solo bastaba con un ordenador y un poco de trabajo, sino que, que requería unos ordenadores de mayor potencia y unos conocimientos más profundos sobre los algoritmos. Poco tiempo después, incluso estos quedaron obsoletos.

Actualmente, obtener Bitcoines utilizando este proceso no es misión imposible, pero sí queda reservado a ordenadores muy especializados y específicos, además de que, este proceso se ha encarecido bastante, llegando incluso a ser más costoso el proceso que el valor del producto final, por lo que, este proceso está casi descartado para aquellos que se planteen obtener Bitcoines por cuenta propia.

La tecnología por tanto, es una de las herramientas fundamentales si escogemos este proceso para crear y obtener Bitcoines. Desde que, por allá 2009, se diera a conocer al mundo Bitcoin, la tecnología que se utiliza para crear esta criptomoneda ha sufrido muchos cambios, ha ido creciendo y evolucionando de la mano de Bitcoin.

Esta evolución comprende desde cuando, en el nacimiento de Bitcoin, crear dicha criptomoneda era tan sencillo como tener, únicamente un ordenador conectado a la red y, desde casa se podía obtener Bitcoines, hasta la actualidad, donde, para crear la criptomoneda, ahora se requiere un *Application Specific Integrated Circuit,* un

circuito integrado para aplicaciones específicas, se trata de unos chips específicamente diseñados y creados para dichas tareas.

Además, los conocimientos que se necesitan hoy en día para minar una criptomoneda no tienen ni punto de comparación, en grado de dificultad y complejidad, a los que se necesitaban en un primer momento, por lo que, hoy en día, la creación de criptomonedas a través de este proceso ha quedado restringido a unos cuantos eruditos o personalidades con recursos muy abundantes capaces de desembolsar todo lo necesario en personal cualificado y los equipos informáticos, además de otros gastos inherentes a estos.

A modo de conclusión, y una vez analizado el proceso de minado, es lógico pensar que, actualmente, no es rentable minar una criptomoneda, ya que existen otros procesos y alternativas mucho más sencillos y económicamente viables que este.

4.1.1.1 Los pools de minería

Un pool de minería hace referencia a la asociación o agrupación de varios mineros independientes en un solo bloque para así aumentar sus probabilidades de encontrar un bloque de Bitcoines.

A modo de ejemplo, esto sería como un sindicato, donde los trabajadores se afilian para proponer cambios y, con el poder de todos trasladarles esos cambios y exigencias a los empresarios, que, de ir individualmente un trabajador directamente al encargado no conseguiría nada, con la fuerza del grupo se consiguen dichas mejoras y alcanzar su objetivo.

Los pools por lo tanto, funcionan de una manera parecida, los mineros se agrupan para trabajar conjuntamente y, con la suma de las probabilidades individuales de cada minero de encontrar un bloque se logra una probabilidad mucho más elevada que si un minero intentará buscar el bloque de forma individual.

Además, estas agrupaciones ofrecen la posibilidad de entrar al proceso de minería a los mineros que, de otro modo, no podrían acceder. Otra de las ventajas que presentan estos pools es que, dada la política que tienen, se incentiva mucho la

competitividad y el trabajo, puesto que cuando logran descubrir un bloque, la recompensa por ello se reparte de manera proporcional entre los mineros de dicho pool, por lo que, aquel minero que más haya aportado en el descubrimiento del bloque, mayor recompensa obtendrá que aquel que ha intervenido en menor medida.

V. LA SEGURIDAD DE BITCOIN: LA CRIPTOGRAFÍA

Actualmente, los distintos métodos de criptografía se pueden dividir en clasificar en uno de estos dos grupos:

- **Criptosistemas asimétricos o de clave pública:** En esta clase de sistema criptográfico se utilizan dos claves distintas, una clave privada y otra clave pública. Una de estas dos se encargará de realizar la función de cifrado de nuestro mensaje, mientras que la otra se encargará del proceso inverso, se encargará del descifrado. Dado que la clave pública es, valga la redundancia, pública es accesible por todo aquel que quiera conocerla, por tanto, esta cumple con una función muy importante e indispensable, y es que está pensada para que resulte imposible derivar de esta la clave privada, por lo que son muy útiles y recomendables para establecer una comunicación segura en un medio inseguro, como lo es Internet, puesto que, y aunque "viaja" por la red pública, si alguien quisiera descifrar el mensaje sin conocer previamente la clave privada, le resultaría imposible de hacerlo.

- **Criptosistemas simétricos o de clave privada:** Esta clase de sistema es algo más sencillo que los anteriores, dado que únicamente requiere una sola clave, tanto para cifrar como para descifrar el mensaje. Por lo tanto, para que el receptor de nuestro mensaje pueda descifrarlo y acceder a él, deberá conocer la clave que he utilizado para cifrarlo, mientras que, con el anterior sistema, tanto emisor como receptor tendrían cada uno su propia clave.

Ambos sistemas comparten una característica común, y es que, tanto los sistemas simétricos como los asimétricos son unidireccionales, estos significa que, el proceso

para cifrar un mensaje es sencillo de hacer, pero el proceso inverso, de pasar del cifrado al descifrado es muy muy complicado. Llegados a este punto se nos plantea una nueva cuestión, entonces, ¿qué nos garantiza la criptografía?.

- **Confidencialidad:** Dado que es un sistema de seguridad, únicamente los usuarios autorizados y conocedores de las claves tendrán acceso a nuestro mensaje y nadie más que ellos.

- **Integridad de la información:** La criptografía, además de garantizarnos que nadie ajeno a quien nosotros queramos tenga acceso al mensaje, esta nos asegura que la información no será alterada por nadie, por lo tanto, la información original que nosotros enviamos será la misma que la que el receptor des encripte.

    - **Autenticación de usuario:** También nos permite verificar que el usuario que pretender acceder a nuestro mensaje es quien dice ser y no un suplantador o impostor.

    - **Autenticación de remitente:** Al igual que la característica anterior, esta nos permite comprobar que el mensaje que recibimos fue enviado, efectivamente por quien dice que envió y no otra persona.

    - **No repudio en origen:** Esto nos garantiza que, una vez se recibe el mensaje, el emisor no puede negar haberlo enviado.

    - **No repudio en destino:** Una vez el mensaje enviado, el receptor de este no puede negar haberlo recibido.

    - **Autenticación de actualidad:** Esta función nos permite verificar que el mensaje que recibimos es actual, y no un mensaje antiguo reenviado.

Puesto que, como hemos comentado anteriormente, los sistemas de criptografía simétrica tienen serias limitaciones, quedan reservadas a un uso entre usuarios más privado (puesto que el emisor debe transmitirle al receptor la clave para que este pueda descifrar el mensaje) y entre dos personas, ya que, si quiero comunicarme

con más, tendré que crear una clave para cada una de ellas (y estas no son cortas ni fáciles de recordar), cabiendo la posibilidad que, con tanta clave diferente, en algún momento se me olvide. Dicho esto, no tendría mucho sentido profundizar en este tipo de sistemas ya que, normalmente, enviaremos mensajes a más de una persona, por lo tanto, pasaremos a analizar los sistemas de encriptación asimétricos y estos los dejaremos como un mero apunte.

5.1 La anonimidad de Bitcoin

A Bitcoin se le han atribuido una serie de cualidades positivas, la gran mayoría de ellas ciertas, aunque también existen otras que, no son cien por cien ciertas o que se han distorsionado un poco para potenciar y ensalzar más esta criptomoneda. Una de estas cualidades que siempre se le ha atribuido a Bitcoin es su total y completa anonimidad, algo que se contrapone con el hecho de que, TODAS las transacciones realizadas con Bitcoin en la red quedan registradas y almacenadas en la cadena de bloques o *blockchain*, que funciona como un libro contable infinito, público y accesible por cualquiera que quiera consultar cualquier transacción realizada.

Por lo tanto, ¿por qué se dice que Bitcoin garantiza nuestra anonimidad? Cuando hablamos de anonimidad, a lo que queremos hacer referencia es a que, lo que Bitcoin permite es el anonimato del usuario que ha realizado una transacción, puesto que, si nos fuera posible conocer quién está detrás de cada operación que se ha llevado a cabo, podríamos rastrear de donde provienen esos fondos. A nadie le gustaría que, una vez realizado un pago, cualquiera pudiera “tirar del hilo” y descubrir de donde provienen esos fondos y por lo tanto, tener acceso y conocimiento de los fondos que tenemos en nuestras cuentas, por lo que, un sistema de pagos nos garantice esta anonimidad parece algo deseable por todo el mundo. Una criptomoneda, por tanto, debería ser capaz de garantizarnos dos cualidades muy importantes:

1. Que no sea rastreable, es decir, que no sea posible de saber quien realizó

una operación.

2. Que no sea vinculable, que se nos garantice que no sea posible conocer para qué se utilizó dicha criptomoneda.

Bitcoin, en un primer momento, parece que reúne ambas características, aunque, si echamos un vistazo más clínico, vemos que no cumple al cien por cien con ellas, por motivos de eficiencia más que nada. El siguiente gráfico es muy esclarecedor y nos permitirá entender de una manera más sencilla todo este tema de la anonimidad y la privacidad en la utilización de Bitcoin:

En el gráfico de la imagen no10, podemos comprobar cómo, cualquier transacción u operación que realicemos con Bitcoin será anónima, pero no privada, puesto que la única transacción que cumpliría con ambas características seria el pago en efectivo.

Para la gente que utiliza Bitcoin con fines, llamemos “normales” o comunes, ser anónimos es importante pero no es algo imperativo, pero, ¿qué pasa con aquellos que utilizan Bitcoin, y aprovechan esta anonimidad, para usos menos legales o “normales”?

Aquí es donde entra en juego la red oscura o Darknet, que es donde normalmente operan estos usuarios que quieren garantizar su anonimato y en donde, es indiferente que método de pago se utilice, dado que cuando se utiliza esta red para realizar operaciones, nuestra anonimidad está garantizada al cien por cien, ya que se oculta la IP de nuestro ordenador y por lo tanto, hace casi imposible el rastrear el origen de una transacción. Por lo que, los detractores del Bitcoin pierden un poco de peso, ya que, aunque Bitcoin sea anónimo, existen algunos métodos para saber quién está detrás de una dirección Bitcoin, mientras que, quienes operan por la red oscura, ya sea con su cuenta de Bitcoin o con una cuenta bancaria normal, su anonimidad sí que estará garantizada, por lo que, los que afirman que Bitcoin facilita este comercio ilegal es porque no está del todo bien informado, o simplemente, quiere desprestigiar o difamar a esta criptomoneda que, en mi opinión, esta llamada a ser el futuro medio de pago global.

Recientemente he leído una noticia en uno de los diarios más populares en España,

el periódico La Vanguardia, que llamó mi atención. En dicho artículo, se utilizaban argumentos como que era una moneda que facilitaba la financiación de actividades ilegales, que se utilizaba para blanquear el dinero obtenido de la droga o tráfico de armas y que, al ser una moneda irrastreable, permitía a los delincuentes mantener su dinero oculto de la ley. Además, argumentaba que, en un momento en el que se está intentando acabar con los paraísos fiscas, Bitcoin ha aparecido como la gran salvadora para todos aquellos que quieren mantener su dinero escondido, llegando a considerarlo un paraíso fiscal 2.0.

En él también se afirmaba que, Bitcoin es CLARÍSIMAMENTE un medio de transacción con fines delictivos y el comercio ilegal. También se daban argumentos a favor de esta criptomoneda, explicando que, en contra de lo que todo el mundo cree, no es 100% anónima, ya que todas las transacciones que se realizan con Bitcoin quedan registradas en la Blockchain, siendo ésta pública para todo el mundo que quiera consultarla, por lo que, como la clave pública es accesible por todo el mundo, cualquiera puede saber cuántos fondos tienes depositados en tu monedero, cuantos has llegado a tener y cuantas transacciones has realizado, por lo que la hace perfectamente rastreable.

Dicho esto, los argumentos en contra de Bitcoin y todos aquellos que lo criminalizaban quedan indefensos y sus argumentos pierden todo el peso que tenían a priori, dado que, esa anonimidad de la que tanto hablan únicamente se aplica a que, en un principio no se sabe quién es el dueño de dicha cartera, la identidad de su propietario sí que queda en el anonimato. Ahora muchos detractores se me echarán encima y atacarán diciendo que eso es la descripción de paraíso fiscal, pero, no tan rápido, como he dicho, A PRIORI, la identidad esta oculta, aunque, actualmente, existen opciones para saber quién es el propietario de dicha cartera , dado que, todo aquel que quiera adquirir Bitcoines y los quiera almacenar en un monedero digital tiene que pasar obligatoriamente por una de las miles casas de cambio que existen hoy en día, en ellas se le pide al usuario la identificación y queda registrado en su sistema, por lo que, si las autoridades lo requiriesen pueden solicitar dicho registro y descubrir la identidad de quien está detrás de ese monedero digital.

VI. LAS BASES DE BITCOIN

6.1 Las cadenas de bloques o *Blockchain*

Una cadena de bloques no es más que un registro de todas las transacciones que se producen en la red, funciona como un libro mayor, de consulta pública y accesible por todo el mundo y compartido por toda una red de ordenadores.

Si Bitcoin funciona hoy en día tan bien y eficientemente es, en gran parte, por la incorporación de la cadena de bloques en su funcionamiento. Gracias a ésta, podemos controlar el dinero, las transacciones que se realizan y hacen imposible que pueda darse la posibilidad de un doble gasto. La información que componen estos bloques se almacena en una estructura de datos, donde encontramos la cabecera de bloque, el cual incluye una referencia al hash (que anteriormente hemos comentado) o resumen del mensaje original, que posteriormente des encriptaremos. Este hash o resumen de nuestro mensaje hace, además, la función de identificador del bloque que lo contiene.

La cadena de bloques nació de la mano de Bitcoin, en enero de 2009. A este primer bloque se le llamó bloque génesis. Este primer bloque equivalía a 50 Bitcoines. El bloque génesis se considera que es el padre de todos los demás bloques que han ido surgiendo desde que este se encontrará en enero de 2009, este es el punto de partida de todos los bloques de cualquier cadena de bloques que analicemos.

Para que quede mucho más claro el proceso y el circuito que sigue una transacción realizada mediante Bitcoin o cualquier criptomoneda pondré un ejemplo que intentaré sea lo más explícito posible para esclarecer y aclarar cualquier duda que pudiera surgir de cómo funciona una operación con este novedoso sistema. A modo de ejemplo, imaginemos que tengo una cartera digital con 3 Bitcoin en ella y quiero realizar una transferencia a un amigo a su cartera digital, entonces, el proceso que seguirá la cantidad de Bitcoin que transfiramos hasta llegar a la cartera de destino es el siguiente:

1. La petición de transferencia que yo realizo llega a los ordenadores conectados a la red de Bitcoin y estos la registran en un bloque, donde

constan todas las transacciones pendientes de realizar, a la espera de ser ejecutadas.

2. Antes de validar y dar el visto bueno a estos bloques que contienen dicho registro de transacciones y queden anotados en la Blockchain, el libro general de cuentas de Bitcoin se debe resolver un reto o problema matemático para que ello se produzca.
3. Así, el primer ordenador que consiga resolver dicho reto matemático será el encargado de validar el bloque del cual ha resuelto el problema y anotarlo en la Blockchain, este hecho recibe el nombre de minar una moneda.
4. Una vez resuelto el problema, validado el bloque y registrado en la Blockchain, todas las transacciones que estaban registradas en el bloque en cuestión se producirán y nuestra transferencia se realizará y le llegará a la cartera de nuestro amigo.

El ordenador que haya sido capaz de resolver el problema matemático y registran el bloque en la Blockchain recibe, a modo de recompensa, una cantidad X de Bitcoin, o de la criptomoneda en cuestión. Resolver dicho reto es muy complicado dado la inmensa cantidad de ordenadores que se encuentran conectados a la red Bitcoin y, por lo tanto, ser el primero en resolverlo es tremendamente difícil.

En la red Blockchain existe una dirección única “A” que pertenece a mí, que soy el que realiza la transacción, y una dirección “B”, de destino, que será la dirección de la cartera digital de mi amigo, el que recibirá mi transacción. También constará en este registro la cantidad de Bitcoin que enviamos y mi firma digital propia, necesaria para poder realizar cualquier transacción con cualquier criptomoneda.

Al no contar con un nodo único y central que gestiona todas las transacciones e información, nos encontramos con una red de nodos, totalmente descentralizados, que son los que se encargan de recopilar todas esas transacciones y juntarlas en un bloque, y ella se encarga de gestionarla y enviarla allí donde se quiera, con la resolución del problema matemático previamente comentado. Dada la inexistencia de un nodo central, cualquiera que quiera, que cuente, claro está, con un ordenador,

puede entrar a operar como nodo en la red Blockchain. El problema de las redes descentralizadas era el de la gestión de datos, ya que tenemos que saber gestionar muy bien esa gran cantidad de datos, y para solucionar y solventar ese problema surgió Blockchain.

Blockchain es muy difícil de alterar o manipular ya que, si se modifica un bloque, como ese cuenta con una copia exacta para cada uno de los nodos, solo tendríamos que comparar los bloques de los nodos para ver que uno es diferente y que por lo tanto ha sido manipulado.

Además, queda totalmente registrada la autoría del remitente, es decir el receptor de una transacción sabe y conoce la identidad de aquel que le ha realizado la transferencia.

Otro uso que se le puede dar a la Blockchain, es el de utilizarla para algo más que realizar transferencia y destinarla para el funcionamiento de las criptomonedas. Se puede utilizar para que, por ejemplo, esos mismos bloques contengan datos, de cualquier tipo, y que por lo tanto, la información quede totalmente descentralizada, ya que se encuentra distribuida por los diferentes nodos de la red y no esté controlada por alguien, como sucede en las redes con un nodo central. Llevado, por ejemplo, al campo de la sanidad, la información que gestiona el sistema sanitario sobre cada uno de sus pacientes, ahora esa información queda almacenada en el servidor de cada hospital, así nuestro expediente médico está distribuido por todos aquellos hospitales los cuales hemos visitado. En Blockchain, podríamos almacenar nuestro expediente, encriptarlo para asegurar dicha información, de manera descentralizada y distribuida por toda la red de ordenadores y, adicionalmente, yo podría decidir quién quiero que vea y tenga acceso a mi expediente, aumentando así la privacidad de uno y teniendo un control sobre quién tiene acceso a qué, y no como ahora, que nadie me asegura que el médico que tiene acceso a mi expediente lo comparta con quien quiera.

Cuando desde una dirección, ya sea de Bitcoin o de cualquier otra criptomoneda, se produce un envío de dinero o transacción a otra dirección. Cualquier transacción que se realice tiene su propia firma digital, con una clave privada. Una transacción se

compone básicamente de dos elementos:

- Input o Entrada: Es el registro que hace referencia al origen de dichos fondos que se están "moviendo".

- Output o salida: Éstas hacen referencia al destinatario de dichos fondos.

VIII. CONCLUSIONES

- El Bitcoin, a pesar de todas sus ventajas y el aire fresco que supone para la economía global y el sistema de pagos y transacciones, sigue siendo un sistema experimental, en constante proceso de mejora.
- Pese a ser la criptomoneda más popular, no es la única, ni la mejor de entre ellas. Existen otras monedas digitales que presentan características que superan a las de Bitcoin u ofrecen servicios más completos.
- Gracias a su naturaleza, es posible introducir mejoras y actualizaciones en las criptodivisas, siempre propuestas, consensuadas y aprobadas por la comunidad, y no manipuladas por algún órgano gubernamental o banco.
- Las criptomonedas nos ofrecen control y gobierno total sobre nuestros fondos, sin necesidad de depender de terceros ni que estos acaben decidiendo sobre nuestro dinero. Uno mismo actúa como su propio banco personal.
- La criptografía protege y asegura nuestros fondos, que, al encontrarse únicamente en la red (las criptomonedas no existen en formato físico a diferencia del dinero fiduciario), entorno inseguro por naturaleza, podría echar para atrás a aquellos escépticos e indecisos de invertir en monedas digitales.
- Si, las criptomonedas finalmente llegan a convertirse en el medio de pago global, facilitarían las transacciones entre individuos de diferentes países o continentes, generarían mayor eficiencia para sus usuarios (que cada vez que viajen a países donde no aceptan su moneda, deban obligatoriamente cambiarla por la moneda correspondiente) y serían de más fácil transporte, ya que como he comentado, no existen en formato físico, únicamente digital.
- Muchas de las críticas que reciben Bitcoin, y las criptomonedas en general,

quedan desmontadas o pierden todo su peso una vez analizamos en mayor profundidad estas monedas digitales, dado que, al tratarse de algo completamente nuevo y diferente, existen muchas incógnitas y desconocimiento sobre éstas.

- Dado que se trata de un sistema tan innovador y no cuenta con unas bases sobre las que operar, considero necesario una especie de "convenio" o "estatutos" aprobados por la comunidad de usuarios y que asienten estas bases y ayuden crear el marco sobre el que se asentarán las criptomonedas. Adicionalmente a lo comentado en la anterior conclusión, dada la falta e inexistencia de unas "bases" y lo "jugosas" que resultan las criptomonedas para los inversores, nos encontramos un producto financiero extremadamente volátil, lo cual complica que se asiente en la economía y que muchos usuarios indecisos frente a ellas la descarten rápidamente por el miedo a estas fluctuaciones tan bruscas.
- La tecnología de la cadena de bloques, Blockchain, representa un mundo totalmente nuevo en cuanto a las posibilidades que nos brinda, y, ahora, depende de nosotros el uso que le queramos dar, la idea es muy buena e innovadora, pero el fin para lo que se use dependerá de nuestros intereses.
- Los detractores de las criptomonedas, refuerzan sus argumentos en contra con el hecho de que, su valor, al contrario de lo que ocurre con el dinero fiduciario, se fija en el mercado, por lo que proviene de la oferta y la demanda que exista en ese momento, mientras que el valor del dinero viene fijado por entidades supra gubernamentales u organismos y no por los usuarios, que son los que al fin y al cabo componen tanto la oferta como la demanda y por lo tanto, el mercado en sí.
- Muchas de las críticas que se le atribuyen a las monedas digitales provienen de entidades financieras u organismos los cuales ven, en esta nueva forma de dinero, un enemigo peligroso y a tener en cuenta, dado que ponen en entredicho su soberanía y forma de proceder y hacer las cosas y se postula como su substituto en la economía.
- La gran variedad de criptomonedas que encontramos en el mercado, esto nos permite una gran flexibilidad en el momento de decidir en que criptodivisa

invierto o adquiero. Por lo tanto, y viendo el brutal incremento de valor que está experimentando Bitcoin, cosa que los pone al alcance de muy pocos bolsillos, podemos optar por opciones y alternativas mucho más asequibles a este, sin tener que ser obligatorio desembolsar una gran cantidad de dinero si queremos invertir en este nuevo producto.

- De seguir con este ritmo de crecimiento tan descontrolado y fluctuando tan bruscamente, el mercado de las criptomonedas acabará explotando y convirtiéndose en el fin de otra burbuja, como a otros activos les sucedió en su momento.
- Hoy por hoy, el futuro de Bitcoin y del resto de criptomonedas resulta incierto, pudiendo dar un giro de 180o en cualquier momento y cambiar la dirección a seguir.
- Para evitar y acabar con el uso criminal que le dan ciertos individuos a las criptomonedas para sus fines ilícitos, habría que acordar y fijar hasta qué punto el uso de una criptomoneda me garantiza mi anonimato y en caso de su uso para financiar actividades ilegales, que mediante algún método, salte una alarma y se le bloquee la cartera al ciberdelincuente en cuestión y que este sea reportado a las autoridades y quede al descubierto.

IX. BIBLIOGRAFÍA

Este artículo se basa en el trabajo de final grado presentado por el primer autor, en los que se destaca las referencias siguientes, entre las múltiples consultadas:

- JUAN MANUEL GONZALEZ OTERO, BITCOIN. LA MONEDA DEL FUTURO UNION editorial s.a.
- SANTIAGO MARQUEZ SOLIS, BITCOIN: GUIA COMPLETA DE LA MONEDA DEL FUTURO, editorial ra-ma
- http://www.lavanguardia.com/economia
- https://www.coindesk.com/price/
- https://www.plus500.es/Instruments/BTCUSD
- https://es.cointelegraph.com
- Cita de Santiago Márquez Solís (2016) en su manual, Bitcoin: guía completa de la moneda del futuro.
- Lex Solokin, economista y a favor de las criptodivisas.[SEP]v Billy Markus, creador de Dogecoin, la criptomoneda satírica.[SEP]v *Wall Street Journal*, diario americano especializado en economía y finanzas.