MEMORIA DEL TRABAJO FIN DE GRADO

Análisis teórico-práctico de la moneda virtual Bitcoin y sus implicaciones económicas

Theoretical-practical analysis of Bitcoin virtual currency and its economic implications

Autor/a: D. Rafael Sánchez Leonsegui

Tutor/a: D. Ginés Guirao Pérez

Grado en ECONOMÍA
FACULTAD DE ECONOMÍA, EMPRESA Y TURISMO
Curso Académico 2017 / 2018

LUGAR Y FECHA
La Laguna, a 11/06/2018

1. RESUMEN Y ABSTRACT

RESUMEN

Es evidente que la popularidad obtenida por Bitcoin debe presentar unas bases racionales que la expliquen, por ello en el presente Trabajo de Fin de Grado (TFG) se pretende realizar un análisis del funcionamiento técnico y las características que muestra Bitcoin. Además, se expondrán los problemas que presenta la moneda, en seguridad criptográfica, legalidad y problemas de escala que nacen por los propios fundamentos de la moneda.

Por otro lado, se realiza un análisis empírico que tratará de dilucidar cuales son las previsiones sobre si Bitcoin cumplirá en última instancia lo que el documento de presentación recogía como principal objetivo de la moneda, que en resumen es servir como sustituto del dinero convencional. Al final del trabajo se expondrán los resultados y conclusiones obtenidas en el desarrollo del mismo, así como algunos aspectos filosóficos y valores que la Fundación de Bitcoin declara como propios.

Palabras clave: Bitcoin, cadena de bloques, criptomonedas, dinero, activo de inversión

ABSTRACT

It is obvious that the popularity obtained by Bitcoin must show some rational basis which explain it, so in this paper we pretend to make a technical analysis about how the virtual currency works, and about the characteristics it puts on the table. Moreover, we will expose the problems the currency face in terms of cryptographic security, legality and scale problems which appear because of the own fundamental properties of the currency.

Later, we will make an empirical analysis which will try to conclude whether if the currency fulfills the main objective of serving as a replace to conventional money written down in the presentation paper or not. At the end of the paper we show our results and conclusion obtained with the investigation, moreover we will show some philosophical aspects and values The Foundation of Bitcoin declare as own.

Key words: Bitcoin, blockchain, cryptocurrencies, money, financial investment

ÍNDICE

2. INTRODUCCIÓN

Bitcoin es una moneda virtual descentralizada cuya creación data de 2008. El documento en el que se presenta el proyecto es firmado por el pseudónimo de Satoshi Nakamoto, aún hoy se desconoce la identidad del creador o creadores.

Tras nueve años de existencia, la moneda digital ha ido ganando una cuantiosa popularidad entre inversores, empresarios y consumidores, experimentando una revalorización sin precedentes sobre todo a partir de 2013. La popularidad obtenida y la funcionalidad que muestra la tecnología que hace funcionar a Bitcoin, la cadena de bloques, han determinado la puesta en marcha de incontables proyectos criptográficos paralelos a Bitcoin y en el presente actuando como competidores directos de la moneda que en este trabajo se estudia.

En 2008 nos encontramos en un contexto internacional de crisis financiera, iniciada con el derrumbe de las hipotecas sub-prime en Estados Unidos, que obligó a los Bancos Centrales a iniciar una política monetaria poco convencional centrada en introducir liquidez en el sistema. La crisis también cuestionó el poder del dinero fiduciario de países de la Europa periférica, desmantelando su aparente solidez.

Esta situación impulsó a un grupo de ingenieros japoneses a presentar su proyecto de dinero digital. A pesar de que anteriormente habían surgido propuestas y proyectos de monedas electrónicas, siempre aparecía el mismo problema, el denominado doble gasto. En otras palabras, sin una autoridad central o un tercero de confianza que se encargue de verificar las transacciones puede surgir el problema de que el mismo dinero sea gastado dos o más veces, creando un caos monetario improcedente.

De este modo, con el impulso suscitado por la crisis surge Bitcoin. En enero de 2009 nace la red Bitcoin tras el minado del primer bloque conocido como “Bloque Génesis” por Satoshi Nakamoto. Éste dejará de ser la cara visible de Bitcoin en 2010, pasando el testigo como tal a Garvin Andresen, en la actualidad cabeza visible del proyecto.

En octubre de 2009 se realiza el primer cambio de Bitcoins por Dólares, con un tipo de cambio de 0,003$/BTC. Unos meses después se realiza la primera compra en Bitcoins, el comprador pagó 10.000 Bitcoins por dos pizzas, en la actualidad esas pizzas habrían costado algo más de 70 millones de dólares.

Tiempo después, Mt. Gox inicia sus servicios como bróker de Bitcoin, para meses más tarde convertirse en el bróker con el mayor número de intercambios con la moneda, y años después quebrar debido al haber experimentado un *hackeo* y robo de millones de dólares en Bitcoins.

A mediados de 2012 se crea la Fundación Bitcoin de la que hablaremos más adelante.

En 2013 Bitcoin llega a oídos del senado estadounidense, cuando el Comité de Seguridad y Asuntos Gubernamentales llevan a cabo el primer debate sobre Bitcoin, sobre lo que deciden no actuar por el momento.

En 2017, tras años de constante subida de precio y popularidad se produce el definitivo boom de la moneda.

Por otro lado, se empiezan a desarrollar *hard forks*, también en 2017. Un *hard fork* en Bitcoin es una bifurcación intencionada del código de Bitcoin que puede tener dos finalidades, por un lado, crear una moneda nueva basándose en el código de Bitcoin, o bien actualizar el código de Bitcoin. Para lo primero no es necesario llevar a cabo ningún proceso democrático que lo autorice, cualquier persona con conocimientos puede hacerlo, sin embargo, una bifurcación intencionada enfocada a actualizar el código del propio Bitcoin si requiere del consenso general, y por ello han sido rechazados en más de una ocasión.

Un *hard fork* puede tener distintos resultados; un cambio en las reglas del sistema, una ampliación o reducción del tamaño de los bloques, etc. En cualquier caso, el cambio ha de ser importante para considerarlo como *hard fork*.

Por el contrario, un *soft fork* se define como una bifurcación del código para actualizar el sistema, de manera consensuada, y que no repercute de manera importante en el funcionamiento de la red.

Por último, es posible encontrar *forks* accidentados, éstos se producen cuando los desarrolladores de la red cometen errores al actualizar el sistema, y para reparar los errores es necesario realizar una nueva bifurcación.

2.1. BREVE HISTORIA DEL DINERO

Para estudiar Bitcoin, primero es preciso llevar la vista atrás para revisar cual ha sido la trayectoria seguida por el dinero a lo largo de la historia. De este modo podremos hacernos una idea con mayor facilidad de si a lo que estamos asistiendo con la creación de Bitcoin y sus "monedas hermanas" puede ser el inicio de algo grande en el futuro o no.

En un primer momento, el dinero tenía la forma de bien material, palpable, con un valor intrínseco propio. Esta clase de dinero mercancía fue el que se impuso tras el trueque, diferenciándose del mismo llanamente en que los bienes con los que se realizaban intercambios eran socialmente aceptados por la mayoría, además servía como unidad de valor para el resto de productos o servicios, es el caso de la sal o el cacao, por ejemplo.

Un ejemplo reciente de esta clase de dinero lo podemos encontrar en las prisiones, es de conocimiento popular el uso que los cigarrillos reciben en ellas como unidad de valor en el proceso de tasación de otros bienes y servicios que los presos intercambian.

Las primeras monedas que se conocen se acuñaron en Lidia, la actual Turquía en el siglo VII a.C. formadas por una aleación de oro y plata debido al elevado valor que la sociedad imponía sobre estos metales preciosos. Las monedas acuñadas llevaban marcas oficiales que garantizaban su valor y autenticidad, de modo que los engaños y las estafas se redujeran al mínimo. Años más tarde, los griegos en la "Edad de Oro de Grecia" se encargaron de perfeccionar estas monedas, dibujando en ellas símbolos sobre todo de índole espiritual en forma de animales y dioses. Con la caída del imperio romano y la consecuente desestabilización europea se entró en una etapa en la que la acuñación de monedas se redujo drásticamente, y con ello el comercio. En el siglo VII d.C. se emiten los primeros billetes de los que se tiene constancia en China, tenían una forma cuadrada

y estaban compuestos de piel de ciervo y bordes de colores. A pesar de las facilidades en el transporte que los billetes concedían, Europa no los introdujo en un principio.

En el renacimiento (1300 d.C.) con el surgimiento de la banca moderna en Italia, se comienza a perfeccionar el papel moneda para que pudiera ser utilizado en el uso cotidiano entre las clases pudientes de la sociedad y facilitara el comercio. A mediados del siglo XV aparecen las letras de cambio, los pagarés, las obligaciones, los cheques y los giros postales.

En el siglo XIX el dinero entra en una etapa en que su valor se determina a escala global a través de un bien común, el oro. La adopción de este sistema fue gradual, y aportó gran estabilidad debido al tipo de cambio fijo y una inflación muy baja, favoreciendo el comercio internacional.

No obstante, en 1971 tras muchos años de decadencia del sistema, EE. UU. cancela unilateralmente la convertibilidad directa del dólar en oro, dando fin al acuerdo de Bretton Woods. A partir de este momento y hasta hoy se entra en una etapa caracterizada por la existencia del dinero fiduciario, carente de valor en sí mismo, pero respaldado por instituciones financieras y Estados que garantizan su valía.

3. DEFINICIÓN Y ASPECTOS TÉCNICOS

Comenzamos definiendo qué es Bitcoin y que cualidades posee. En este sentido se podría decir que se asimila al dinero electrónico convencional con la diferencia de que Bitcoin no representa a una moneda preexistente (como euros o dólares), sino que tiene su propia unidad de valor.

A diferencia del resto de sistemas de dinero digital previos a Bitcoin, éste destaca por ser la primera moneda, electrónica o no, completamente descentralizada. Bitcoin posee las características del dinero electrónico, pero el hecho de utilizar una *red peer-to-peer* (P2P)[1] y ciberseguridad la encaja en la subcategoría de criptomoneda.

El conjunto de monedas criptográficas no se limita a conceder garantías de seguridad en las transacciones, sino que poseen características comunes que determinan la filosofía de este tipo de dinero de reciente creación:

- La oferta de dinero está controlada por un algoritmo del que hablaremos más adelante, su funcionamiento es de dominio público y es independiente de la política monetaria de los bancos centrales
- La verificación de las transacciones es descentralizada y no jerárquica
- Las carteras electrónicas no están directamente relacionadas con sus dueños en términos de información identificativa, lo cual concede al consumidor altos niveles de anonimato, aunque no es total.

De acuerdo con lo anterior, podemos definir a Bitcoin como una criptomoneda descentralizada, pseudo-anónima, alternativa al dinero digital convencional y que forma parte del sistema de pago *peer-to-peer*, basándose además en un protocolo criptográfico que utiliza un algoritmo para regular la oferta de la moneda.

[1] Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

El principal reto que surge en la elaboración de un sistema descentralizado de pagos electrónicos sin intermediarios es el problema del doble gasto, es decir, que el mismo dinero no sea gastado más de una vez. En el dinero electrónico convencional este problema se solventa con la existencia de una institución financiera de confianza que se encargue de verificar la veracidad de las transacciones, impidiendo el doble gasto. Sin embargo, en la tecnología *Blockchain* (cadena de bloques)[2], se crea un libro de contabilidad totalmente público donde se registran todas y cada una de las transacciones llevadas a cabo con la moneda. Son los propios usuarios los que se encargan de verificar las transacciones y aceptarlas como correctas, en el momento en que se confirma una transacción como correcta, ésta no puede ser cancelada.

Los usuarios de Bitcoin utilizan carteras electrónicas que almacenan los datos digitales necesarios, permiten crear direcciones y gestionar los saldos de bitcoin asociados a determinadas direcciones. Las direcciones de bitcoin se asemejan a cuentas bancarias con la diferencia de que en las primeras es posible conocer la cantidad monetaria que hay en una cartera, pero no la identidad del dueño. Para autorizar las transacciones cada dirección posee una clave privada y otra pública, siendo la primera la que se utiliza para hacer efectiva la tentativa de transacción. Cada transacción se registra en bloques conformados por alrededor de 2000 de ellas y no son más que archivos de texto con información. Estos bloques son elaborados por los denominados "mineros" que con la ayuda de un software especializado y utilizando su propia energía eléctrica y computacional, solucionan el problema criptográfico que verifica la transacción (la prueba de trabajo[3]). Cada bloque generado contiene un *hash*[4] del bloque anterior, de modo que todos los bloques se encuentran interconectados directa e indirectamente dando lugar a lo que se conoce como la cadena de bloques.

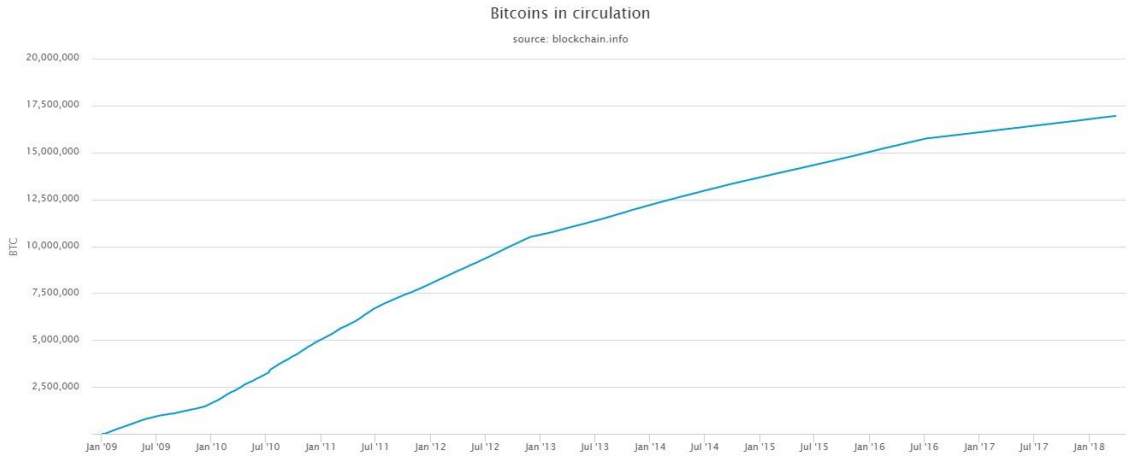
Teniendo en cuenta el coste en energía, software y tiempo necesario para generar nuevos bloques, los mineros son recompensados cada vez que generan un bloque correcto con bitcoins que se añaden al mercado, aumentando la oferta monetaria. En un principio la recompensa era de 50 bitcoins, actualmente de 25 bitcoins por bloque. Esto es así porque la cifra máxima de bitcoins emitidos ha de ser de 21 millones de monedas, y para controlar la emisión se manipula la recompensa de modo que sea cada vez menor, al mismo tiempo, generar un bloque nuevo aumenta de dificultad progresivamente, reduciendo con ello la creación de nuevas monedas. Se estima que en 2032 se habrá emitido el 99% de la oferta máxima posible de bitcoins, y en 2040 la totalidad de bitcoins estará en el mercado.

[2] Una cadena de bloques o cadena articulada, conocidas en inglés como blockchain, es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metainformación relativa a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas la información contenida en un bloque sólo puede ser repudiada o editada modificando todos los bloques posteriores.

[3] Prueba de Trabajo, o PoW (por sus siglas en inglés), es el algoritmo de consenso original en una red de Blockchain. En la Blockchain, este algoritmo se usa para confirmar transacciones y producir nuevos bloques en la cadena.

[4] Las funciones hash criptográficas son aquellas que cifran una entrada y actúan de forma parecida a las funciones hash, ya que comprimen la entrada a una salida de menor longitud y son fáciles de calcular. Se llaman funciones hash criptográficas a aquellas funciones hash que se utilizan en el área de la criptografía.

1. Total de Bitcoins minados hasta enero de 2018

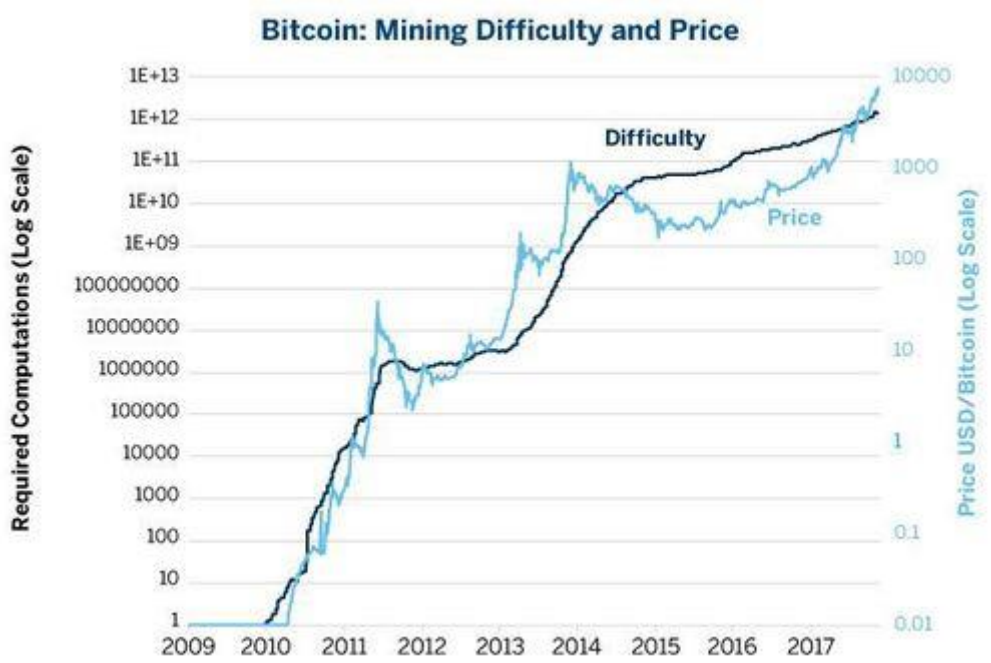


Fuente: Blockchain.info

Un tema controvertido sobre la tecnología bitcoin es el supuesto anonimato que la moneda confiere al tenedor. Bien, esto no es del todo real, en todo caso se podría hablar de un pseudo-anonimato, ya que, aunque si es cierto que en el registro de la cadena de bloques no hay nombres ni apellidos, sí encontraremos direcciones IP de los ordenadores que dan la orden para que una transacción se lleve a cabo, es por ello por lo que cualquier persona con conocimientos informáticos sería capaza de rastrear y encontrar al usuario que actuara malintencionadamente.

Para que minar no resulte tarea sencilla y de este modo cualquiera pueda sacar beneficios del sistema, la red Bitcoin tiene una dificultad de bloque global. Es decir, los bloques válidos deben tener un *hash* con una dificultad inferior a ese límite global. La dificultad cambia cada 2016 bloques, basándose en el tiempo que se tardó en descubrir los anteriores bloques. En el caso de que cada bloque se resuelva cada 10 minutos, como en primera instancia se quiso, encontrar 2016 bloques tomaría dos semanas. En el caso de que los anteriores 2016 bloques se resolvieran en más de dos semanas, la dificultad disminuiría, y viceversa. Además, dependiendo de cuánto más o menos se tarde en resolver los 2016 bloques, la dificultad se incrementará en mayor o menor medida.

2. Dificultad en el minado de Bitcoin y su precio

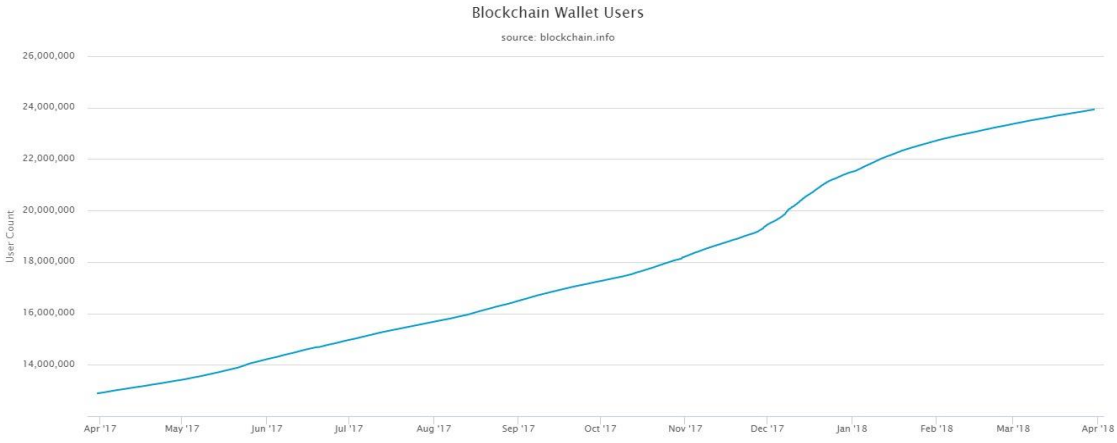


Fuente: Bitcoinwiki.org

4. EL MERCADO DE BITCOIN

Es difícil medir el tamaño de la comunidad de bitcoin debido a su pseudo-anonimato, una opción sería sumar el número de monederos electrónicos creados y en funcionamiento, el problema es que un usuario generalmente posee más de una cartera electrónica, por tanto, este método no sería del todo representativo. A pesar de esto, se estima que alrededor de 10 millones de usuarios interactúan en la red bitcoin diariamente, llevando a cabo una cantidad de transacciones bastante grande, y que ha ido incrementándose desde la aparición de la moneda.

3. El número total de Blockchain Wallet creadas (2017-2018)

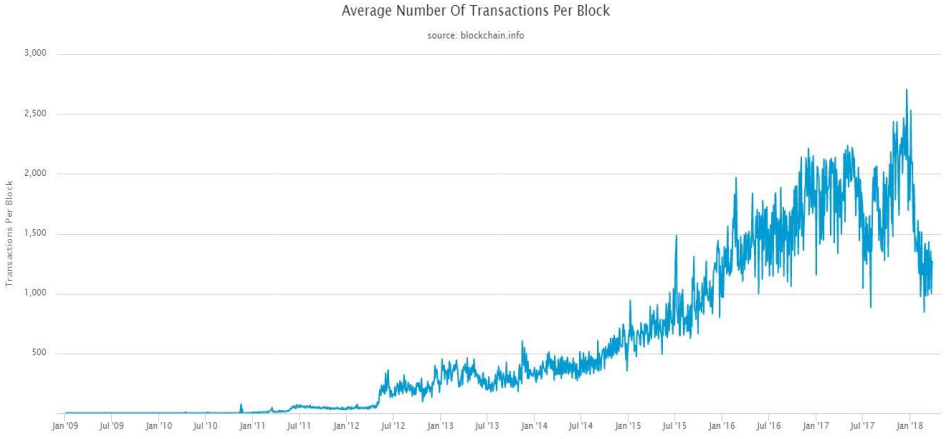


Fuente: Blockchain.info

De este enorme y veloz crecimiento surge un problema de escala que tiene su raíz en el inmovilismo de la base de código que rige la moneda, es decir, la base de código sigue siendo muy similar a como era hace nueve años, y el tamaño del mercado, sin embargo, ha aumentado mucho. Por ello, el crecimiento en el número de usuarios, y con ello del número de transacciones diarias, nos encontramos con que, en su estado actual la red de Bitcoin no puede procesar con la velocidad necesaria todas las transacciones requeridas.

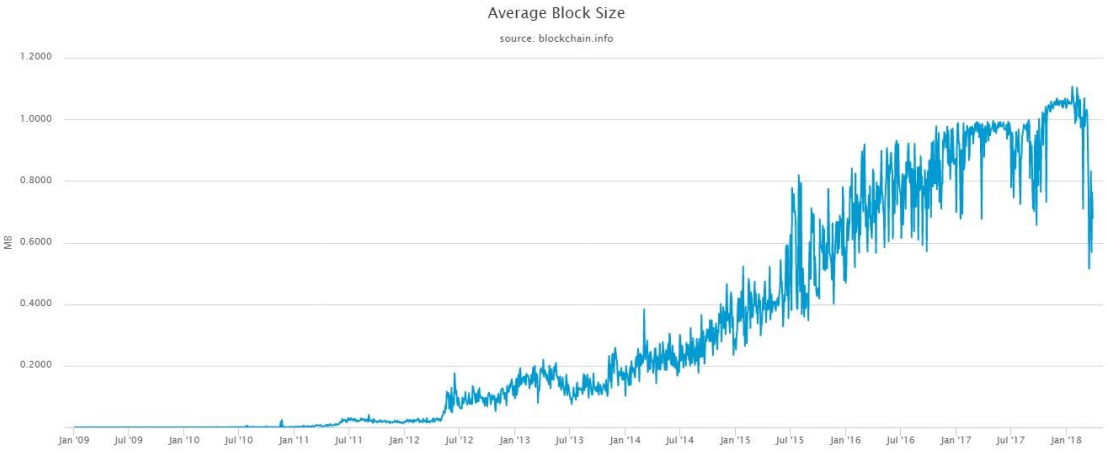
El problema surge debido al límite de tamaño de bloque restringido a como máximo un MB, siendo rechazados como no válidos aquellos bloques que presenten un tamaño superior. Esta característica fundamental de la tecnología bitcoin se estableció para evitar ataques potenciales de piratas informáticos que creaban bloques de gran tamaño, incluso infinitos, para paralizar la red. No obstante, esta medida en la actualidad lo que hace es restringir el número de transacciones por segundo que conforme la comunidad va aumentando, y la tendencia así lo marca, la necesidad de soportar cada vez más transacciones en menos tiempo es crucial para que la red sea eficiente y fructífera. El problema es que la limitación en el tamaño de cada bloque a un MB, circunscribe el número de transacciones por segundo a entre tres y siete.

4. El número promedio de transacciones por bloque (2009-2018)



Fuente: Blockchain.info

5. Tamaño de bloque promedio en MB (2009-2018)



Fuente: Blockchain.info

La implicación directa de esta situación es que, en días extraordinarios en los que la red recibe una inmensa cantidad de solicitudes para llevar a cabo transacciones, ésta se satura de tal modo que ha habido usuarios reportando tiempos de espera de horas en incluso días enteros. Los usuarios pueden acelerar el tiempo de aceptación de sus transacciones compitiendo en el pago de comisiones a los mineros de modo que sus transacciones se procesen primero, sin embargo, esto no hace más que agravar la situación de bitcoin en tanto el aumento de la red incrementa el tiempo de espera para procesar transacciones y con ello se crea un mercado de comisiones que a priori va en contra de la filosofía inicial de la moneda. De aquí surge la pregunta: ¿para qué utilizar la tecnología bitcoin teniendo a las convencionales transacciones bancarias?

Un rol fundamental en el sistema bitcoin lo llevan a cabo los proveedores de servicios de pago. A pesar de que son los bancos los que poseen el papel clave en el pago con tarjeta tradicional, en el mercado del comercio electrónico (e-Commerce) son los servicios de pago no bancarios los que han ido ganando mayor importancia (PayPal, Click2Sell, y un largo etcétera) en las dos últimas décadas. Esto se debe principalmente a la simplificación de la interface, facilitando y animando al consumidor a comprar por vía electrónica. Al contrario ocurre con Bitcoin, para los empresarios, la aparente complejidad que suscita la inserción de la moneda como medio de pago ha ahuyentado a un gran número de empresas. A esto hay que sumarle el riesgo asociado a la fluctuación del precio de la moneda, que desde su creación ha sufrido grandes idas y venidas. Por ello, con el paso del tiempo han aparecido numerosos startups dedicadas a facilitar el pago con bitcoins, llevando a cabo el procesamiento de la transacción y asumiendo el riesgo de la fluctuación. Son estos startups las que más han aportado al crecimiento de la comunidad de bitcoin y de las criptomonedas en general.

Para comprar bitcoins existen casas de cambio (Exchange platforms[5]) cuya tarea no es otra que la de intercambiar unas divisas por otras, cobrando una comisión. Los intercambios de divisas por bitcoins no se registran en la cadena de bloques. Estas casas de cambio no están legalmente reguladas de modo que ante cualquier ataque malintencionado o situación de bancarrota el consumidor no estaría cubierto de ningún modo. Desde que surgió bitcoin, algunas casas de cambio han sufrido problemas graves, como por ejemplo el colapso de la "Exchange platform Mt. Gox" con pérdidas de hasta 450 millones de dólares y dejando a sus clientes sin opción a recuperar el dinero que tenían depositado en ella. Esta y otras situaciones similares han llamado a la regulación del mercado, no solo por lo anterior, sino también para reducir o evitar la evasión de impuestos y blanqueo de dinero, facilitado por el pseudo-anonimato.

4.1. PROBLEMAS POTENCIALES DE LA RED BITCOIN

Se ha evidenciado que tanto Bitcoin, como las casas de cambio (el ejemplo más llamativo es el de Mt Gox) son vulnerables ante potenciales ataques informáticos. En el presente apartado explicaremos algunos de ellos.

Las carteras electrónicas no vienen encriptadas por defecto, por ello éstas se convierten en vulnerables ante cualquier tipo de ataque hacia ellas por la función que cumplen como reserva de monedas.

Reestablecer una copia de una cartera antigua con su contraseña puede ser tarea fácil con un programa de restauración estándar, como por ejemplo Apple Time-Machine. De este modo, restaurar una antigua cartera con su correspondiente contraseña se traduce en restaurar la actual, con el riesgo de poder ser robada.

El conocido como *Sybil attack,* en seguridad informática este tipo de ataque ocurre cuando un sistema distribuido (como la red p2p de Bitcoin) es corrompido por una misma entidad que controla la mayoría de los nodos de la red, de modo que otros usuarios solo puedan conectarse a bloques creados específicamente para llevar a cabo un fraude. El proceso sería como sigue:

- El atacante bloquea las transacciones de otros usuarios, sacándolos de la red.
- Éste solamente deja que la comunidad se conecte a los bloques creados malintencionadamente en una red paralela, y como consecuencia las transacciones aceptadas incurrirán en el problema del doble gasto.

Otro problema importante al que se ha enfrentado Bitcoin desde su creación es al problema del 51%. Este fallo del sistema se podría dar en el caso de que un usuario poseyera un poder computacional superior al del resto de usuarios de la red en conjunto, es decir, más de un 50% del total en manos de una sola persona o grupo aliado. Debido a la democratización por la que se rige la aceptación de los bloques esto sería nefasto para la red, pudiendo llegar a confirmar bloques propios y con ello obteniendo el rendimiento de manera corrupta. En todo caso, si alguien se hiciera con el poder de más del 50% de la red podría actuar de la manera siguiente:

- Cancelar transacciones
- Bloquear el reenvío de transacciones
- Cambiar la cantidad de monedas emitidas en la aceptación de un bloque
- Crear monedas desde cero
- Comprometerse a enviar monedas que no son de su propiedad, etc

Además de los mencionados anteriormente, Bitcoin se enfrenta a los denominados Ataques de Denegación de Servicios (DoS son sus siglas en inglés). Este tipo de ataque informático se basa en el envío masivo de información "basura" a los nodos que trabajan para confirmar las transacciones, dificultando la actividad sobremanera. A pesar de que las versiones más recientes de Bitcoin tienen integradas herramientas para bloquear nodos[6] y transacciones sospechosas, el desarrollo de softwares maliciosos cada vez más difíciles de contrarrestar dificulta requiere de medidas cada vez más costosas.

Por otro lado, la red Bitcoin se puede ver afectada por errores que causarían inestabilidad en la protección del sistema. Teniendo en cuenta que la información en la red ha de actualizarse en el menor periodo de tiempo posible, si debido a un error, ésta no se actualiza, pero aún así sigue entrando información de otros nodos en la cadena, los datos incorrectos comenzarían a propagarse pudiendo llegar a paralizar la red durante horas o incluso días. No obstante, las versiones más recientes de los clientes de Bitcoin (donde se almacena la cadena de bloques, pesando cerca de 70 GB) contienen herramientas que los hace reaccionar de manera rápida y eficaz ante los posibles errores que surgen en la red.

En cuanto a potenciales vulnerabilidades de la red Bitcoin en el futuro debemos mencionar las siguientes:

- Hackeo de la función hash: Los algoritmos para calcular la versión de la función hash que en la actualidad utiliza Bitcoin se presume imposible de hackear con la potencia computacional existente. Sin embargo, en un futuro próximo es posible que se desarrollen ordenadores con una potencia computacional superior, incrementando el riesgo de hackeo de estas funciones, aunque siempre es posible reemplazar la versión actual por una de mayor dificultad.
- Incremento del número de usuarios: A pesar de que Bitcoin se encuentra potencialmente preparado para un incremento cuantioso en el número de usuarios, en el caso de que éstos de forma masiva se inclinara por la utilización de software orientado a la ocultación de sus direcciones ips, la red comenzaría a presentar problemas en su funcionamiento, y habría que desarrollar algún método para contrarrestar esta tendencia.

5. BITCOIN, ¿DIVISA O ACTIVO DE INVERSIÓN?

Popularmente se conoce a Bitcoin como moneda virtual, sin embargo, en las ciencias económicas la definición del dinero ha tendido hacia el funcionalismo, y es por ello por lo que generalmente se considera dinero a todo aquello que cumple las tan conocidas tres funciones:

- ✓ Medio de cambio
- ✓ Unidad de cuenta
- ✓ Depósito de valor

Teóricamente, si Bitcoin es utilizado fundamentalmente como divisa para el intercambio de bienes y servicios, competiría con el dinero fiduciario tradicional, influyendo en su valor y afectando a las políticas monetarias que implementaran los bancos centrales.

En el caso de que fuera utilizado principalmente como activo de inversión, éste competiría con una gran cantidad de activos existentes, como los bonos del tesoro o las mercancías subyacentes en contratos de futuros.

De este modo, el éxito de Bitcoin como moneda o como activo de inversión depende de su capacidad para competir con lo ya existente, y en el apartado que sigue vamos a realizar un análisis de las capacidades de la divisa electrónica para comprobar en qué destaca actualmente, y a qué aspira.

5.1. BITCOIN COMO MONEDA

Con la creación de Bitcoin se pretendía en un principio, y así viene recogido en el documento emitido por su creador para introducir su funcionamiento, que se estableciera como un potencial sustituto del dinero fiduciario en el que se basa el intercambio en la actualidad.

En este respecto, la teoría económica funcionalista dicta que para que algo pueda ser considerado dinero ha de cumplir tres funciones fundamentales, esto es, medio de cambio, unidad de cuenta y

depósito de valor. En el presente apartado estudiaremos si realmente Bitcoin cumple o no dichas funciones.

a. Medio de cambio

La teoría dicta que un bien funciona como medio de cambio cuando éste es aceptado por todos en la compraventa de bienes y servicios, pagar deudas o impuestos, etc, y para ello ha de cumplir determinadas propiedades.

En primer lugar, ha de ser fácilmente transportable. El dinero fiduciario lo es en pequeñas cantidades, así como el electrónico en forma de tarjetas de débito y crédito. En este sentido Bitcoin no tiene ningún problema más allá de poseer una buena conexión a internet para poder llevar a cabo las transacciones.

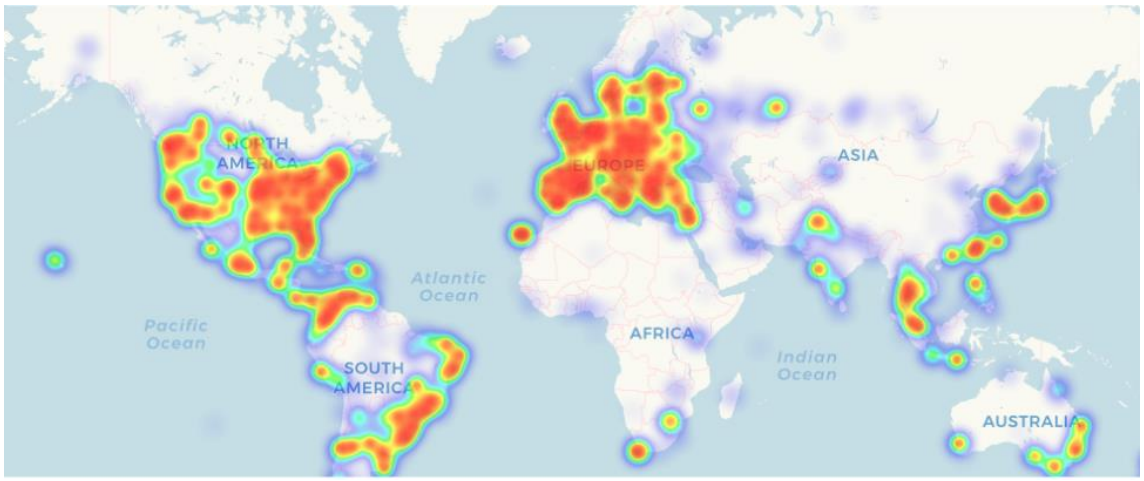
En segundo lugar, el dinero ha de ser divisible si pretende servir como medio de cambio. Bitcoin lo es hasta 0,00000001 BTC (conocido popularmente como un Satoshi).

La siguiente propiedad con la que nos encontramos es la de la mutua equivalencia entre divisas, es decir, que una unidad de dinero sea equivalente a otra en su valor y aceptación. El primero de los puntos los cumple, pues la convertibilidad de Bitcoin en cualquier otra moneda viene dada por el mercado de divisas en su conjunto. Sin embargo, la segunda de las propiedades no es cumplida ya que no existe una aceptación generalizada alrededor de la moneda, a pesar de que la aceptación ha ido creciendo progresiva y constantemente desde su creación, ésta dista de ser generalizada. En conclusión, el poder de Bitcoin, al igual que ocurre con otras monedas, radicará en el poder de la red y usuarios que lo utilicen.

Por el lado empresarial se observa un aumento de la aceptación del Bitcoin como pago con el paso del tiempo. La ausencia de comisiones o costes adicionales en el uso de Bitcoin en contraposición a, por ejemplo, las tarjetas de crédito, es un gran atractivo para los empresarios, sobre todo aquellos que representan el sector de las pequeñas y medianas empresas con bajos márgenes de rentabilidad.

Coinmap estima que unas 12274 empresas aceptan Bitcoin como medio de pago, no obstante, se presume que la cifra sea superior, pues en la web solo aparecen las empresas registradas en la misma. A continuación adjuntamos un mapa de calor que muestra los comercios que aceptan Bitcoin en todo el mundo.

6. Comercios que aceptan Bitcoin - Abril 2018



Fuente: Coinmap.org

La progresiva adopción de bitcoin como medio de cambio en una cantidad respetable de empresas lleva a pensar que la tecnología representada por bitcoin es lo suficientemente positiva como para darle una oportunidad.

Como se ha comentado con anterioridad, el principal beneficio de su uso es la reducción de los costes en el proceso de pago. Sin embargo, en contraposición nos encontramos con la extrema volatilidad de la moneda. Es por ello por lo que aquellos empresarios que deciden aceptar el pago en bitcoins suelen desarrollar políticas encaminadas a minimizar la exposición al riesgo del tipo de cambio de bitcoin. Como es lógico, los empresarios buscan que la volatilidad en los precios de los bienes en venta sea inferior a la de bitcoin, para ello establecen los precios en moneda fiduciaria tradicional, y de ese modo se minimiza la volatilidad visible de los precios. Además, se encargan de actualizar constante y regularmente los precios de los bienes en bitcoins, con el fin de obtener el beneficio acorde a lo que obtendría si la venta se llevara a cabo mediante cualquier moneda tradicional.

Entonces, para el consumidor ¿es más rentable comprar con bitcoins o con cualquier otra moneda? Para responder a esta pregunta, haremos referencia a un trabajo empírico desarrollado por la Reserva Federal de Boston. Para el estudio se escogen dos bienes, en este caso un USB Kingston y un Iphone 5C, de dos tiendas electrónicas que aceptan el pago en bitcoins y en dólares (Overstock y TigerDirect).

En el estudio se observa que el precio en dólares de los bienes varía poco o nada a lo largo del periodo estudiado, mientras que en el caso de los precios en bitcoins, éste solo se mantiene válido durante cortos periodos de tiempo, en el caso de Overstock es actualizado cada diez minutos, y en el de TigerDirect, cada 15 minutos.

Los resultados demuestran que la compra en bitcoins conllevaría un descuento ínfimo que depende del tipo de cambio utilizado. Además, se observa en las regresiones simples desarrolladas por los investigadores que durante periodos en los que los precios ostentan una mayor volatilidad el descuento en las compras con bitcoins en comparación con el dólar son mayores.

Aparte de la volatilidad, otro problema que los empresarios tienen en cuenta al decidir o no aceptar Bitcoin como medio de pago es el del tiempo necesario para que el bloque concreto que contenga la transacción requerida sea aceptado, en el caso de pequeñas cantidades, la transacción se valida rápidamente tras su notificación a la red, sin embargo, cuando las cantidades en la transacción son mayores, el tiempo varía y puede llegar a alcanzar una hora.

b. Unidad de cuenta

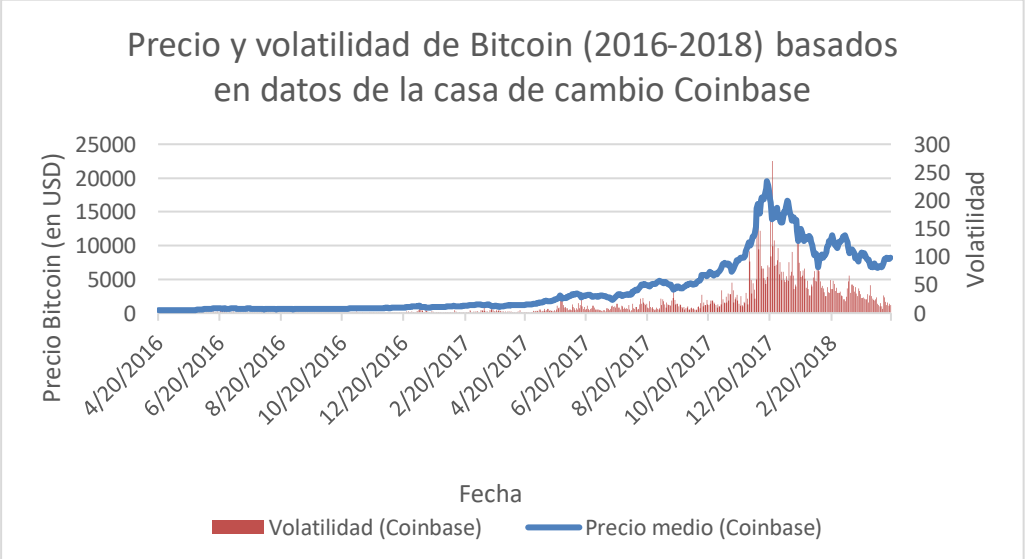
Otra función del dinero es la de servir como unidad de cuenta, es decir, la de ser usado como referencia para fijar el precio de bienes y servicios de muy distinta índole. Al medir el valor de las cosas basándose en el precio de la moneda como referente, se simplifica el sistema de precios relativos y se reducen los costes de información.

Sin embargo, como se comentó con anterioridad, la enorme fluctuación de los precios de Bitcoin no capacita a la moneda para servir como unidad de cuenta.

En la terminología financiera se define a la volatilidad como una medida de la variabilidad del precio de un activo a lo largo del tiempo. En otras palabras, cuando hablamos de la volatilidad, nos estamos refiriendo a la cantidad de incertidumbre o riesgo que existe sobre el tamaño de los cambios en el valor de un activo financiero concreto. Una elevada volatilidad significa que el precio de un activo puede cambiar dramáticamente en un corto periodo de tiempo, una baja volatilidad alude a que el valor del activo financiero en cuestión no va a fluctuar demasiado, pero sí podría variar en un periodo de tiempo prolongado. Para medir la volatilidad en el precio de Bitcoin se ha recurrido a la media de la desviación típica calculada cada hora durante el periodo elegido.

El gráfico siguiente muestra una correlación positiva entre el precio de Bitcoin y la volatilidad registrada a lo largo del periodo elegido (desde abril de 2016 hasta febrero de 2018).

7. Precio y volatilidad de Bitcoin (2016-2018)



Fuente: Data.bitcoinity.org. Elaborado por el autor.

La extrema volatilidad en el valor de Bitcoin en comparación con otras monedas es un obstáculo enorme en la consideración de ésta como una herramienta útil de unidad de cuenta. El hecho de que su valor se dispare o reduzca en periodos de tiempo muy cortos obliga a los comerciantes que aceptan Bitcoin como medio de pago a actualizar los precios de los productos cada poco tiempo, siendo esto una práctica que hace incurrir al empresario en costes innecesarios y al consumidor en confusión.

Por el lado de la inversión (que se traslada al ámbito empresarial y del consumo comentando en el párrafo anterior), por ejemplo, una persona que hubiera invertido 1.000 EUR en Bitcoin al cierre de 2016 (cuando su valor rondaba los 1.000EUR/BTC) habría obtenido un rendimiento del 1.000% en menos de un año, pues a mediados de noviembre de 2017 el valor de la moneda se situaba en los 11.000 EUR/BTC. Sin embargo, a final de mes el valor de la moneda cayó hasta cotizar en 9.000 EUR/BTC, por tanto, una persona que hubiera invertido 15.000 EUR en el pico histórico hasta entonces, a finales de noviembre habría sufrido unas pérdidas virtuales de 2500 EUR aproximadamente.

Más acuciada fue la caída del precio de Bitcoin a final de 2017, después de haberse incrementado desde los 1.000 EUR/BTC hasta cerca de 20.000 EUR/BTC. A finales del año pasado, la moneda pasó de valer, en menos de dos meses, de los 20.000 EUR/BTC mencionados con anterioridad a unos 7.000 EUR/BTC. Todo esto se debe a dos motivos fundamentales:

El primero es el desconocimiento generalizado sobre la moneda, alcanzando una popularidad aceptable a lo largo de 2017, pero sin destacar excesivamente. El hecho de que la tecnología que mueve a Bitcoin es incomprendida por un amplio segmento de la sociedad, y sumado a esto, de muy reciente creación hacen que su valor sea difícil de precisar.

Además, hay que tener en cuenta que la gran mayoría de los Bitcoins minados hasta hoy pertenecen a un grupo pequeño de personas, a finales de 2017 sólo 1.000 personas controlaban el 40% del total de los Bitcoins minados hasta el momento, de manera que si los tenedores decidieran liberar grandes cantidades de Bitcoins al mercado su valor se desestabilizaría por completo. No obstante, la extrema volatilidad no es el único ni más importante problema de la moneda a la hora de actuar como unidad de cuenta, además nos encontramos con el elevado coste relativo de un Bitcoin comparado con el de otras monedas, induciendo a empresarios a vender sus productos en Bitcoin con precios de cuatro o más decimales, de nuevo causando confusión al consumidor. En la economía actual lo normal es encontrar casos contrarios a esta situación, generalmente debido a una elevada inflación, por ejemplo esto es lo que ocurre en el caso Venezolano, a día de hoy 1 EUR valdría 73.149 Bolívares.

c. Depósito de valor

Otra función del dinero, remarcada por Keynes en sus críticas a la teoría clásica es que ha de servir como depósito de valor, es decir, ha de mantener su valor a lo largo del tiempo para poder adquirir bienes y servicios con él en el futuro.

Para que un bien cumpla la función de depósito de valor debe de estar dotado de determinadas características. En primer lugar, tiene que ser duradero en el tiempo en el sentido del deterioro.

Bitcoin al ser un bien electrónico no sufre desgaste alguno, ni por el paso del tiempo ni por situaciones puntuales como podrían ser un incendio, una inundación, etc. Además, como se comentó anteriormente tampoco padece problemas de escala para ser guardado o transportado.

Sin embargo, otra propiedad importante es la de conservar un valor estable a lo largo del tiempo, y como se explicó en el apartado anterior, Bitcoin no destaca en la actualidad precisamente por esto. De este modo, mantener Bitcoins incluso a lo largo de periodos cortos de tiempo conlleva un gran riesgo e incertidumbre.

Por otro lado, el hecho de que la oferta de Bitcoins esté limitada a 21 millones de unidades teóricamente evitaría cualquier situación de espiral inflacionaria generada por la impresión masiva de dinero en un determinado momento. Pero paradójicamente lo que previsiblemente ocurriría cuando Bitcoin fuera notablemente aceptado por todos los agentes de la economía sería lo opuesto, es decir, ante una oferta limitada de Bitcoin y una demanda cada vez más grande de los mismos, el precio se dispararía, los poseedores decidirían mantener los Bitcoin ya que cada vez tendrían una capacidad de compra mayor, y los precios de bienes y servicios se reducirían. En otras palabras, la economía entraría en una espiral deflacionaria caracterizada por precios de bienes y servicios por debajo de lo normal, el precio de bitcoin desmesuradamente elevado, deudores perjudicados por el valor creciente de sus deudas en bitcoin, y en consecuencia, la actividad económica y la confianza se verían deterioradas de tal modo que se entraría en una importante recesión.

5.2. BITCOIN COMO ACTIVO DE INVERSIÓN

Bitcoin se presenta como un híbrido entre el “dinero mercancía” y el “dinero fiduciario” en tanto es escaso debido a su diseño, que limita su oferta total en 21 millones de unidades, en este sentido se asimila al “dinero mercancía” como puede ser el oro, escaso por naturaleza y descentralizado. Por otro lado, Bitcoin, al igual que el dinero fiduciario no posee valor intrínseco al contrario de lo que ocurre con el oro y otros activos considerados como “dinero mercancía”.

Si nos detenemos a evaluar el uso potencial y la futura aceptación de Bitcoin debemos tener en cuenta lo que conlleva que la oferta de la moneda virtual sea limitada y predecible como consecuencia de lo anterior. Dado que la demanda de Bitcoins es impredecible en contraposición a su oferta, es complicado realizar una estimación acerca del valor y usos que se le van a conceder en el futuro. No obstante, que la demanda siga creciendo es ciertamente probable, y en ese caso llegará un momento en que la demanda será superior a la oferta con lo que esto significaría, incremento del precio de la moneda y como consecuencia, efectos deflacionarios en la economía, todo esto en el supuesto de una aceptación generalizada como medio de pago de Bitcoin.

En el caso de que Bitcoin fuera progresivamente aceptado como medio de cambio y se convirtiera en una alternativa al dinero fiduciario, se daría una dualidad basada en la coexistencia de dinero fiduciario y moneda virtual debido al carácter internacional de Bitcoin, dependiendo de la regulación propia de cada país acerca de su uso. La historia nos ha mostrado casos en los que ha existido una coexistencia entre dinero fiduciario y dinero mercancía en un mismo país, como por ejemplo en la década de 1930 en Estados Unidos eran admitidos como medio de pago billetes emitidos por bancos privado al mismo tiempo que los emitidos por la Reserva Federal. Otro

ejemplo interesante es el de Suiza, un país desarrollado en el que circulan simultáneamente Euros y Francos Suizos. No obstante, es más fácil encontrar casos similares en economías de países emergentes como Cuba, Liberia o varios países latinoamericanos.

La ley de Gresham establece que cuando coexisten dos monedas diferentes en un país, reguladas y aceptadas de igual forma, pueden ser definidas como "buenas" o "malas", dependiendo de si la diferencia entre el valor nominal y el real de la moneda es mayor o menor. Cuando esto ocurre, en palabras de Gresham, la moneda "mala" desplazará de la economía a la "buena", ya que la segunda tenderá a ser guardada como depósito de valor. Sin embargo, en los tiempos actuales hemos asistido a una "dolarización" en países con economías y monedas más débiles, lo cual se contrapone con lo que Gresham definió. En este sentido, explica Mundell que en el largo plazo es más probable que las monedas consideradas "buenas" desplacen a las "malas" que lo opuesto.

Para dilucidar si Bitcoin se comporta en mayor medida como moneda orientada a servir como medio de cambio o si por el contrario actúa como activo de inversión dedicado a la especulación vamos a llevar a cabo un análisis estadístico basado en los retornos de Bitcoin y los distintos tipos de usuarios que conforman la red Bitcoin:

Tabla 1. Activos que se comparan con Bitcoin

Variable	Explicación	Tipo de activo
bitr	índice de tipo de cambio de Bitcoin	Moneda virtual
sp5r	Índice de acciones de EEUU (S&P500)	Acciones
sp6r	Índice de acciones de EEUU (S&P600)	Acciones
gldr	Precio oro	Metal precioso
silvr	Precio plata	Metal precioso
eurr	Tipo de cambio entre Euros y dólares	Moneda
audr	Tipo de cambio entre Dólar Australiano y USD	Moneda
jpyr	Tipo de cambio entre Yen y USD	Moneda
gbpr	Tipo de cambio entre Libra Esterlina y USD	Moneda
cnyr	Tipo de cambio entre Yuen Chino y USD	Moneda
hufr	Tipo de cambio entre Florín Húngaro y USD	Moneda
twus	Índice del peso del USD con respecto a otras monedas	Moneda
wtir	Índice del petróleo	Energía
hhr	Índice del gas natural	Energía
cbr	Índice de bonos corporativos de Bloomberg en los Estados Unidos	Bono
tbr	Índice de Bonos del Tesoro de Estados Unidos de Bloomberg	Bono
hbr	Índice de bonos corporativos de alto rendimiento Bloomberg USD	Bono

En primer lugar, presentamos la evolución de los retornos de Bitcoin durante el periodo escogido para el análisis 2010-2015 en USD. En el gráfico se observa en términos generales un incremento de la rentabilidad considerable y una volatilidad muy elevada.

La siguiente tabla muestra algunas estadísticas descriptivas (media, desviación típica, simetría y curtosis) sobre los retornos de Bitcoin comparados con los de otras clases de activos. Se ha utilizado datos diarios entre julio de 2010 y junio de 2015.

Tabla 2. Estadísticas descriptivas sobre los retornos de Bitcoin

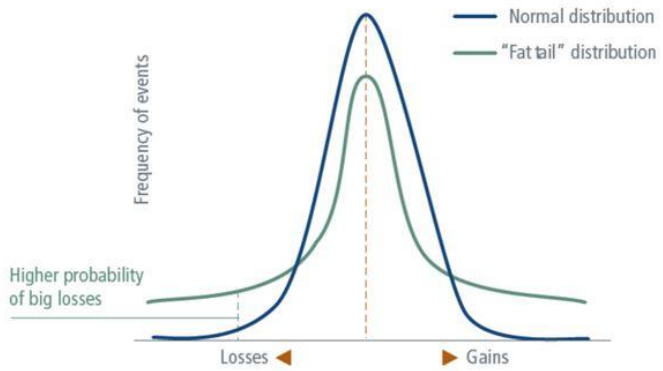
-	bitr	sp5r	sp6r	gldr	silvr	eurr
Media	0,65%	0,05%	0,06%	0%	-0,01%	-0,01%
Desviación típica	7,60%	0,95%	1,27%	1,09%	2,20%	0,60%
Asimetría	-1,01	-0,49	-0,24	-0,89	-0,89	-0,32
Curtosis	17,04	8,25	7,64	10,85	12,94	4,79
-	**jpyr**	**gbpr**	**cnyr**	**hufr**	**twus**	**wtir**
Media	0,03%	0%	-0,01%	0,02%	0,01%	-0,03%
Desviación típica	0,58%	0,47%	0,13%	0,93%	0,29%	1,23%
Asimetría	0,38	-0,06	0,05	0,17	0,29	-0,64
Curtosis	8,22	3,63	13,56	4,36	5,97	9,16
-	**cbr**	**tbr**	**hbr**			
Media	0,01%	0,01%	0,03%			
Desviación típica	0,05%	0,27%	0,18%			
Asimetría	-0,31	-0,17	-1,92			
Curtosis	4,98	3,77	17,58			

Bien, para definir cualquier distribución es posible utilizar dos estadísticos básicos como son la media y la desviación típica, la media nos dice dónde se encuentra el peso de la distribución, y la desviación típica la manera en la que ésta se distribuye. Es por ello por lo que al medir la rentabilidad de un activo financiero es importante fijarse en la volatilidad expresada mediante la desviación típica. Además de las dos variables anteriores, existen otras que también son interesantes y funcionales para el análisis, por ejemplo, el estadístico Curtosis que mide el nivel de concentración de observaciones en la media de la distribución. Ante una Curtosis elevada podremos afirmar que los datos de la distribución se concentran en gran medida en la media y a su vez, aunque en menor medida, muy alejados de ésta. El coeficiente de Curtosis puede ser utilizado en muchos casos para determinar observaciones anómalas en la distribución. Por último, es importante medir la asimetría de la distribución para hacernos una idea de la forma de la misma, que en general tiende a ser asimétricamente negativa en cuanto a activos financieros se refiere.

La tabla muestra que Bitcoin presenta mayores niveles de retornos y volatilidad (representada por la desviación típica) que el resto. Asimismo, la volatilidad en los retornos de Bitcoin es superior a la del precio del oro en dólares en el mismo periodo (2010-2015). Por otro lado, los retornos de Bitcoin presentan una asimetría negativa bastante elevada, similar a la de los del oro, la plata o los bonos corporativos de alto rendimiento. Además, los rendimientos de Bitcoin presentan un muy elevado Curtosis, favoreciendo la aparición de riesgo de cola en los retornos de Bitcoin.

El riesgo de cola no es más que la mayor probabilidad de que los rendimientos de una distribución se sitúen en la parte izquierda de la misma, caracterizada por rentabilidades más bajas. En una distribución normal, los rendimientos de mayor probabilidad se concentran en el centro, mientras que en los extremos se concentrarían los rendimientos “menos esperados”.

7. Riesgo de cola



Fuente: rankia.com

En cuanto a la correlación entre los retornos de Bitcoin y las demás variables elegidas para el análisis se observa que no están correlacionados o presentan una correlación muy baja con todos ellos. Los resultados se presentan en la siguiente tabla.

Tabla 3. Correlación entre Bitcoin y el resto de activos analizados

Correlación	bitr	sp5r	sp6r	gldr	silvr	eurr	audr	jpyr	gbpr	cnyr	bufr	twus	wtir	hhr	cbr	tbr	hbr
bitr	1	0.05	0.05	0.04	0.02	0.01	-0.02	0.01	0.01	0.02	-0.01	-0.01	0.01	0.00	-0.01	-0.03	0.05
sp5r		1	0.92	0.05	0.04	0.15	0.18	0.06	0.14	-0.03	-0.20	-0.41	0.36	0.01	-0.06	-0.48	0.32
sp6r			1	0.06	0.05	0.12	0.14	0.04	0.10	-0.02	-0.16	-0.37	0.32	0.00	-0.08	-0.45	0.24
gldr				1	0.81	0.33	0.38	-0.24	0.34	-0.14	-0.29	-0.29	0.05	0.06	0.04	-0.03	0.06
silvr					1	0.33	0.42	-0.12	0.34	-0.15	-0.32	-0.29	0.09	0.07	0.06	-0.04	0.14
eurr						1	0.55	-0.22	0.65	-0.24	-0.80	-0.51	0.14	0.05	0.07	-0.12	0.16
audr							1	-0.22	0.50	-0.20	-0.59	-0.55	0.18	0.03	0.10	-0.15	0.32
jpyr								1	-0.21	0.09	0.09	0.25	-0.04	-0.03	-0.02	-0.05	0.06
gbpr									1	-0.21	-0.57	-0.43	0.15	0.05	0.05	-0.13	0.20
cnyr										1	0.20	0.21	-0.02	-0.11	0.00	0.05	-0.04
bufr											1	0.48	-0.16	-0.03	-0.06	0.15	-0.24
twus												1	-0.37	-0.06	-0.19	0.15	-0.31
wtir													1	0.12	-0.03	-0.24	0.19
hhr														1	-0.01	-0.04	-0.01
cbr															1	0.64	0.25
tbr																1	-0,12
hbr																	1

La tabla muestra casos de correlación positiva entre diferentes activos, como por ejemplo entre la libra esterlina y el euro, la plata y el oro o los bonos corporativos y los del tesoro de EEUU, todos ellos marcados en verde. Asimismo, se observa que algunas variables se encuentran negativamente correlacionadas presentando valores inferiores a -0,5 y con ello una moderada relación inversa entre ellas, algunos de los ejemplos vienen marcados en amarillo en la tabla. Una elevada correlación positiva significa que existe una relación fuerte entre los activos que se encuentren correlacionados, y por tanto, ante subidas en el precio de uno de ellos, es de esperar subidas en el precio el otro activo.

Como se comentó anteriormente, en el caso de Bitcoin encontramos una total ausencia de correlación entre la moneda y cualquier otro activo analizado. Este resultado dota a Bitcoin de una gran utilidad para servir como activo diversificador de la cartera de valores del inversor.

Por otro lado, Dirk G. Baur, KiHoon Hong y Adrian D. Lee (2015) analizaron los distintos tipos de usuarios que conforman la red Bitcoin para responder a la pregunta que pretendemos resolver en este apartado, ¿se comporta Bitcoin como una moneda o como un activo de inversión?.

Para ello, se divide el total de miembros de la comunidad en cinco grupos diferenciados:

- Inversor acivo: Ha realizado más de dos transacciones y en cuantías superiores a los $2.000.
- Inversor que solamente recibe Bitcoins: Usuarios que han realizado más de dos transacciones, y solo recibe Bitcoins en cuantías superiores a los $100 sin enviar Bitcoin, o que ha recibido una sola transacción en cuantía superior a los $100.
- Usuario enfocado al uso de Bitcoin como moneda: Ha realizado más de dos transacciones, tanto recibiendo como ofertando Bitcoins y son de valor inferior a $2.000 cada una.
- Híbrido: Resto de usuarios.
- "Tester" o usuario que prueba el uso de Bitcoin, ya sea en forma de inversión o de compra de bienes o servicios, realizando solamente una transacción inferior a los $100.

Para analizar el comportamiento de los usuarios de la red, se eligen tres momentos concretos (31/12/11, 31/12/12 y 28/12/13) y se estudia el peso de cada uno de cada uno de los tipos de usuarios en el total de Bitcoin ofertados hasta el momento.

Tabla 4. Peso de cada grupo de usuarios en el total de Bitcoins emitidos hasta 2011

	2011			
	Cantidad Bitcoin (en mill.)	Valor en Dólares	% de participación	Nº de usuarios
Inversor activo	0,29	1,38	3,64	18.940
Inversor pasivo	1,66	7,84	20,63	32.996
Híbrido	2,78	13,11	34,49	425.347
Usuario moneda	0,41	1,94	5,1	31.780
Minero	2,76	13,02	34,23	93.304
Tester/Usuario de prueba	0,15	0,73	1,91	118.338
Total	8,05	38,02	100	720.705

Tabla 5. Peso de cada grupo de usuarios en el total de Bitcoins emitidos hasta 2012

	2012			
	Cantidad Bitcoin (en mill.)	Valor en Dólares	% de participación	Nº de usuarios
Inversor activo	0,28	3,73	2,62	82.621
Inversor pasivo	2,46	32,96	23,16	86.304
Híbrido	4,39	58,82	41,34	1.529.848
Usuario moneda	0,74	9,89	6,95	116.986
Minero	2,58	34,58	24,3	119.010
Tester/Usuario de prueba	0,17	2,31	1,63	256.072
Total	10,62	142,29	100	2.190.841

Tabla 6. Peso de cada grupo de usuarios en el total de Bitcoins emitidos hasta 2013

	2013			
	Cantidad Bitcoin (en mill.)	Valor en Dólares	% de participación	Nº de usuarios
Inversor activo	0,52	376,11	4,27	1.035.596
Inversor pasivo	3,64	2630,26	29,86	319.988
Híbrido	5,43	3928,32	44,59	4.044.719
Usuario moneda	0,27	198,19	2,25	464.397
Minero	2,17	1568,6	17,81	135.187
Tester/Usuario de prueba	0,15	107,65	1,22	722.451
Total	12,18	8809,13	100	6.722.338

La tabla muestra que los inversores activos, pasivos e híbridos han aumentado su participación en el total a lo largo del periodo, mientras que los usuarios enfocados al uso de Bitcoin como medio de cambio, mineros y usuarios que entran en la comunidad para probar el sistema han experimentado una caída en el peso total.

El grupo dominante es el denominado como híbrido, pasando de un 34% a un 45% de participación en el mercado de Bitcoin entre 2011-2013, lo cual era previsible ya que el grupo está formado por una mezcla del resto de tipos de usuarios analizados.

Por otro lado, se observa un incremento bastante notable en el grupo de inversores pasivos en detrimento de una disminución en el de los mineros, lo cual lleva a pensar que los segundos tienden a vender o intercambiar las monedas que consiguen como precio por la minería. Además, cabe resaltar el número de usuarios encuadrados en el grupo de inversores pasivos, que siendo en 2013 el que presenta la segunda menor cantidad de usuarios, ostenta la segunda plaza en términos de participación en el mercado (Bitcoins/Población total). Este hecho explica que la utilidad que este grupo confiere a Bitcoin se fundamenta en su conservación orientada al uso como activo de inversión y no como medio de pago de bienes y servicios.

En cuanto al conjunto que ha disminuido su participación en el total del mercado de Bitcoin en el periodo elegido cabe resaltar la caída de los usuarios que dedican Bitcoin como medio de intercambio, entre 2012-2013 pasó de un 6,95% a un 2,25%, facilitando de nuevo la conclusión obtenida en el apartado anterior que determina una clara tendencia por parte del usuario medio a utilizar Bitcoin como activo para la especulación y obtención de rendimientos.

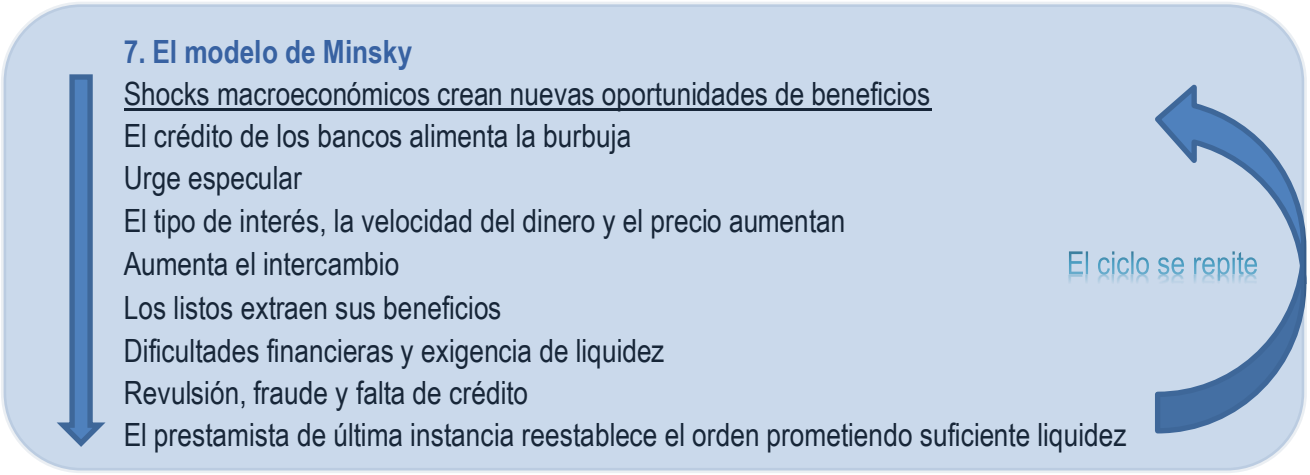
7. LA BURBUJA DE BITCOIN

Anteriormente se comentó que Bitcoin incrementó su valor en $11.000 a lo largo de 2017, llegando a conseguir un valor unitario de $20.000, en los meses posteriores y hasta hoy, su valor no ha hecho más que caer, no obstante, situándose en cifras ampliamente superiores a las registradas a principios del año pasado.

Warren Buffet, considerado como uno de los más grandes inversores a escala mundial, expuso en noviembre de 2017 en la revista Forbes su posición contraria a la moneda Bitcoin alegando que "la burbuja va a explotar pronto". En este sentido, no solo Warren Buffet se posiciona en contra de la moneda, sino que otros muchos economistas de prestigio como Stiglitz, Krugman o Shiller se posicionan del lado de la posible burbuja que se está generando con Bitcoin, llegando a calificar a Bitcoin como "un fraude que debería ser prohibido".

Una burbuja puede ser definida en pocas palabras como una situación en la que el precio de un activo excede su valor real en un margen cuantioso. Con esto extraemos que una burbuja recoge dos variables elementales, precio y valor.

Uno de los estudiosos de mayor reconocimiento por sus aportes en el apartado de las crisis y sus estadios fue Hyman Minsky, economista estadounidense del siglo pasado. En sus investigaciones encontramos el conocido "Modelo Minsky", que recoge nueve estadios en los ciclos de prosperidad y crisis financiera, se expone en la figura siguiente:



Unos años después de la publicación del modelo Minsky, Charles Kindleberger, economista estadounidense experto en historia económica y economía internacional, elaboró un modelo circular sobre las etapas que se atraviesan durante la expansión de una burbuja económica basándose en el modelo Minsky, lo podemos ver representado en el siguiente esquema circular:

En la actualidad, de los estudios centrados en este respecto podemos destacar los desarrollados por Jeremy Grantham, que en resumen vienen a definir una burbuja como movimientos de dos desviaciones típicas del promedio a largo plazo del mercado, en precio/beneficios.

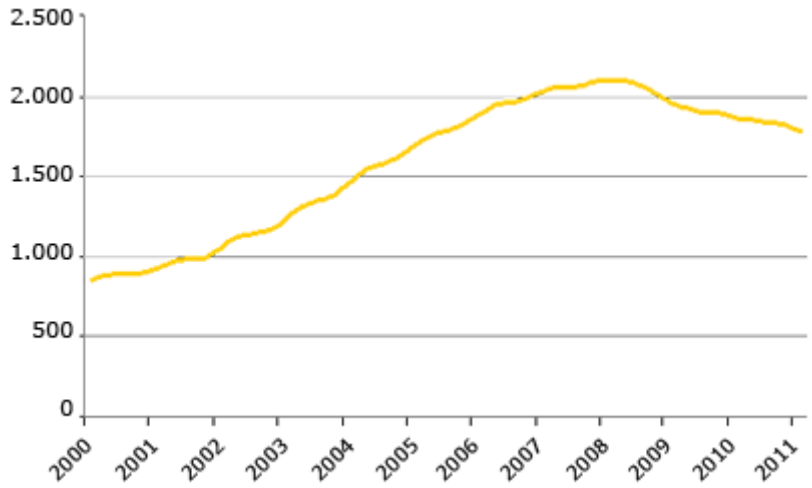
En palabras de Grantham, "las condiciones necesarias para que una burbuja se forme son dos. Primero, las condiciones económicas básicas deben parecer excelentes. Segundo, la liquidez ha de ser generosa en cuantía y precio: debe ser barato y fácil sacar rentabilidad".

7.1 ANALIZANDO EL MODELO KINDIEBERGER-MINSKY: ¿ESTÁ BITCOIN SUFRIENDO UNA BURBUJA?

8. Modelo Kindleberger-Minsky

En el modelo se observan cuatro fases fundamentales por las que pasa una burbuja, primero la fase invisible en la que pocos inversores y agentes de la economía participan en la compraventa del producto que se estudia, la fase de toma de conciencia que sugiere un incremento del conocimiento y aceptación del activo, con la consecuente creación de expectativas positivas y por ende se comienza a invertir en él. La tercera fase es denominada como la fase de manía, en este momento es cuando la popularidad ganada y las expectativas creadas alrededor del activo son sobredimensionadas y se forma, en un contexto de engaño y contagio colectivo, la burbuja. Por último, observamos la fase de liquidación, en la que la confianza se halla mermada por las falsas expectativas creadas de forma masiva durante la fase anterior, y con ello el precio del activo vuelve a su precio medio. Si comparamos la progresión seguida por el precio de Bitcoin desde su primera valoración en 2009 con la forma y las etapas definidas en el modelo Kinderberger-Minsky, se averigua cierta relación entre ellos. Ocurre lo mismo si observamos la progresión de los precios de vivienda en términos nominales antes, durante y después de la burbuja inmobiliaria en España.

9. Evolución de los precios nominales de la vivienda en España (Base 1995)



Fuente: Banco de España

10. Precio de Bitcoin en USD (2009-2018)

Fuente: Blockchain

Según Seaborn Hall en su artículo titulado "Why Bitcoin is not in a bubble", se expresa un punto de vista contrario a la existencia de una burbuja en Bitcoin. En primer lugar, expone que Bitcoin no se encuentra en la fase de liquidación según el modelo Kinderberger-Minsky dado que el precio de Bitcoin ha sufrido reducciones de un 50% en más de una ocasión, y alega que lo que está ocurriendo en la actualidad se debe en gran medida al pánico que las noticias sobre Bitcoin están creando en todo el mundo. En este sentido, Hall establece que la bajada de precio en cerca de $9.000 desde principios de año es una corrección propia de la moneda solo que ha sido acrecentada por el cuantioso valor conseguido a finales de 2017.

Del mismo modo rechaza que Bitcoin se encuentre en la fase de euforia. En la fase eufórica de la burbuja de las punto.com, el valor combinado de todas las acciones de empresas tecnológicas en el Nasdaq era superior, en marzo del 2000, al PIB de un gran número de naciones.

Parece que la posibilidad de que Bitcoin se encuentre en la fase de "Boom" es lo más probable. Coinbase, una importante casa de cambio electrónica, reporta en la actualidad aproximadamente 250.000 registros semanalmente en su página web. Aparentemente, la escasa cantidad de inversión relativa al conjunto de activos financieros explica que Bitcoin y en general las criptomonedas se encuentran efectivamente en una fase de crecimiento temprano, siendo el valor total de inversión en Bitcoins aproximadamente de 500 mil millones de dólares y el del total de activos alrededor del mundo de 80 billones de dólares, representando la inversión en Bitcoin un 0,625% del total.

8. MARCO LEGAL

- Unión Europea: La UE no ha tomado medidas regulatorias concretas en relación al estatus de Bitcoin como moneda, no obstante, sí se ha pronunciado en materia tributaria, imponiendo el pago de IVA (IGIC) y otros impuestos en transacciones realizadas con Bitcoin. Sumado a esto, en 2015 el Tribunal de Justicia de la Unión Europea dictaminó que el cambio de monedas tradicionales basadas en el sistema fiduciario por unidades de Bitcoin está exento de IVA. De esta manera se considera a Bitcoin como medio de pago.

De acuerdo con el Banco Central Europeo (BCE), la regulación del sector financiero no es aplicable a la tecnología Bitcoin porque no involucra actores financieros tradicionales. Por otro lado, el BCE clasificó a Bitcoin como "una moneda virtual descentralizada convertible", aconsejando a bancos la no utilización de la misma hasta que hubiera un marco regulatorio firme.

En 2016 se propuso en el Parlamento Europeo crear un grupo de trabajo para controlar el blanqueo de dinero y el terrorismo financiado por monedas virtuales. La propuesta fue elevada a la Comisión Europea con resultados positivos.

- Estados Unidos: La Comisión de Comercio de Futuros de Productos Básicos clasificó al Bitcoin como un producto básico en 2015, según el Servicio de Impuestos Internos estadounidense, Bitcoin es tratado como una *commodity*, como el oro o el petróleo.

- China: En China, el mantenimiento e intercambio de Bitcoins entre individuales está permitido, sin embargo, la regulación prohíbe que instituciones financieras como los bancos hagan lo propio.

  En febrero del año pasado, varias casas de cambio electrónicas paralizaron el servicio de extracción de Bitcoins, dicha paralización se debió a acciones tomadas por el Banco Popular de China. El BPC ha mostrado su reticencia hacia la moneda desde su creación. A principios de este año, el Banco Popular de China anunció que tomaría medidas drásticas contra la minería de Bitcoin.

Bitcoin y las criptomonedas en general no se encuentran sometidas en la actualidad a una regulación clara ni mucho menos definitiva en ningún país o grupo de países, no obstante, se espera que este proceso regulatorio se lleve a cabo en los próximos años, determinando el futuro de la moneda.

9. LA FUNDACIÓN DE BITCOIN

La fundación es una entidad sin ánimo de lucro estadounidense, creada en 2012 con el objetivo de "estandarizar, proteger y promover el uso de la criptomoneda Bitcoin para el beneficio de los usuarios". Sus documentos fundacionales declaran que los miembros originales son Gavin Andresen, Charlie Shrem, Roger Ver, Mehul Puri, Patrick Murck, Peter Vessenes y Mark Karpeles.

Este apartado tiene la intención de aportar el punto de vista que los acérrimos seguidores de la moneda defienden como si de un dios se tratara, para ello vamos a resumir brevemente lo que el manifiesto de la Fundación declara:

En primer lugar, se enumera una serie de preceptos en los que los miembros de la Fundación creen como ciertos:

- El dinero fiduciario no ha cumplido con la función de depósito de valor, sobre todo después de la abolición del patrón oro
- La inflación fomenta el consumo y desalienta el ahorro y el uso sostenido de los recursos naturales

- Los servicios financieros tradicionales, especialmente la banca, no se encargan de incluir a los 1400 millones de personas que viven en pobreza en el mundo
- El procesamiento del pago electrónico presenta tiempo y tarifas muy elevadas, es por ello por lo que el 85% del comercio global se sigue realizando en efectivo
- El colapso financiero de 2008 resultó en una miseria sustancial para la parte más pobre de la población mundial
- Las pérdidas asociadas al fraude con tarjeta sumaron una cuantía de 16,3 miles de millones de dólares en 2014, más de la mitad ocurriendo online
- La banca tradicional y los sistemas de pago tradicional no son seguros
- La confianza en el sistema financiero tradicional está en su punto más bajo de la historia

Como podemos observar, la Fundación rechaza enérgicamente el sistema financiero tradicional, y en especial a la banca. Además, parece que se posicionan en favor de la pobreza, aunque esto pueda ser moralmente cuestionable por lo que implica para los desarrolladores, ya que, ¿quién no se posicionaría a favor de la pobreza cuando puedes obtener un beneficio de ello?

Por otro lado, en el manifiesto también se expresan los derechos financieros que todo humano debe tener, sin ser coartados por ningún gobierno o ente central:

- El derecho a la privacidad en las transacciones que no implican daño alguno a otros
- El derecho a mantener o gastar tus ahorros en cualquier parte del mundo
- El derecho a participar en la actividad económica con o sin una cuenta bancaria
- El derecho a participar en la actividad económica con o sin historial crediticio
- El derecho a convertir dinero fiduciario en Bitcoin y viceversa
- El derecho a usar Bitcoin como medio de cambio
- El derecho a utilizar Bitcoin como depósito de valor

Todo lo enumerado parece legítimo a priori, no obstante, los dos últimos puntos hablan de derechos que la propia moneda ha de ganar con su propio desarrollo, buen funcionamiento y capacidad de solucionar problemas.

Los valores que defiende la fundación son los siguientes: Privacidad, acceso financiero garantizado, descentralización, autonomía, oferta de dinero estable e inclusión financiera.

10. CONCLUSIONES

Bitcoin es una moneda electrónica descentralizada que se crea en 2008. Su funcionamiento se basa en la tecnología de la cadena de bloques, que no es más que un libro de contabilidad compartido entre todos los usuarios de la red.

Bitcoin, como máximo representante de esta tecnología, así como por ser la moneda criptográfica pionera en introducirlo, ha ganado una popularidad sin precedentes traducida en incrementos cuantiosos en su precio. Todo esto no hace más que presentarnos serias dudas sobre su valor real y hasta qué punto es representado por el precio de mercado sobre el que se mueve la moneda.

Es evidente que la moneda, sobre todo la tecnología *blockchain* muestra unas características únicas, funcionales y revolucionarias, no obstante, no es conveniente caer en el error de sobrevalorar algo por ser nuevo, desconocido y se muestre de gran utilidad.

Aparte de su valor y popularidad ganada, es importante entender que la moneda presenta una serie de vulnerabilidades, tanto potenciales como ya sufridas que hay que conocer si se desea entrar a invertir o comprar Bitcoins para darle el uso que sea. La cadena de bloques al fin y al cabo es un registro contable de todas las transacciones con Bitcoin puede sufrir ataques que se han mencionado a lo largo del trabajo, y, por tanto, a pesar de que la probabilidad de que algo de eso ocurra no es muy elevada, es crucial saber que puede pasar y por qué. Lo mismo ocurre cuando tienes dinero en un banco, has de saber que ese banco puede presentar dificultades de liquidez en algún momento y afectar negativamente al cliente.

En otro orden de cosas, el hecho de que Bitcoin se creara inicialmente con el deseo de convertirse en un potencial sustituto del dinero convencional, encontramos que esto no es así. Si bien su volatilidad, limitación en la aceptación como medio de pago, popularidad limitada a pesar del gran incremento experimentado en los últimos años, el hecho de que la mayoría de los tenedores de Bitcoin han mantenido las monedas durante más de un año en sus carteras, etc. explican que Bitcoin ha tendido a ser utilizado más como activo de inversión que como medio de cambio.

Por el lado de la inversión, al estudiar las características de Bitcoin en comparación con otros activos relevantes y a su vez analizando el comportamiento de cada tipo de usuario, llegamos a la conclusión de que nos encontramos ante una activo que presenta claras diferencias con el resto de los tradicionales. Su precio no está correlacionado con el de ningún activo analizado, ya sean monedas, mercancías o activos financieros. Esta situación favorece enormemente la utilización de Bitcoin como medio para diversificar la cartera de activos de inversión.

En cuanto a los tipos de usuarios de Bitcoin nos encontramos con que un tercio del total de monedas en circulación durante el periodo analizado se encontraban en manos de inversores pasivos, y como consecuencia, tanto el número de usuarios, como la cantidad de Bitcoins utilizados como medio de intercambio es ínfima sobre el total. Este hecho explica que Bitcoin, en el periodo de estudio se dedicaba en gran medida a la inversión y especulación, en detrimento de ser utilizado como unidad de cambio.

Otro tema que se ha tratado en el trabajo ha sido la existencia o no de una burbuja en Bitcoin. Es crucial tener en cuenta las palabras de grandes economistas de la talla de Krugman o Stiglitz

totalmente en contra de la moneda, invitando a los gobiernos a su prohibición, no obstante esta posición contraria no se encuentra respaldada por un trabajo desarrollado con datos empíricos por estos economistas, y por ende no goza de la veracidad científica que se requiere para el trabajo, a pesar de la calidad del resto de su bibliografía.

Lo que sí conocemos con certeza es los modelos elaborados por Minsky y Kinderberger sobre las fases por las que atraviesa la economía cuando experimenta una burbuja, y aunque hay diversas opiniones sobre el tema, Bitcoin por la trayectoria de su precio muestra claras señales de haber atravesado una burbuja y encontrarse en un fase de liquidación, aunque el impacto de la burbuja no ha sido demasiado fuerte dada la escasa capitalización de Bitcoin en el mercado de activos financieros.

11. BIBLIOGRAFÍA (En orden alfabético)

Charles P. Kindleberger (1978) Manias, Panics, and Crashes: A History of Financial Crises

Chris Burniske y Adam White (2017.) Bitcoin: Ringing the bell for a new asset class

Cointelegraph (2017) ¿Qué es un hard fork?

Dirk G. Baur, Ki Hoon Hong, Adrian D. Lee, (2017). Bitcoin: Medium of Exchange or Speculative Assets?

Eashan Kaw (2015). Chinese Geopolitical Strategy and Bitcoin

Héctor Acuña (2017) Estudio sobre Bitcoin y la tecnología *Blockchain*

Hyman P. Minsky (1978) The Financial Instability Hypotesis

Javiflo (2016). El riesgo de cola más presente que nunca

Jeremy Grantham (2018) Bracing Yourself for a Possible Near-Term Melt-Up

Jerry Brito y Andrea Castillo (2013). Bitcoin, manual básico (para legisladores y diseñadores de políticas)

Luis Antonio García Alejo y Ángel Luis Sánchez Lázaro (2016). Bitcoins, documentos electrónicos para el intercambio de bienes y servicios.

M. Beatriz Mota Aragón (2006). El efecto Fisher y el premio al riesgo en México.

Michal Polasik, Anna Piotrowska, Tomasz Piotr Wisniewski, Radoslaw Kotkowski, Geoffrey Lightfoot (2014). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry.

Palacios, Z.J., Vela, M.A. y Tarazona, G.M. (2015). Bitcoin como alternativa transversal de intercambio monetario en la economía digital.

Richard Borsuk (2013) "China Bitcoin Arbitrage Ends as Traders Work around Capital Controls."

Rober Greer (1997). “What is an Asset Class, Anyway?”

Rodrigo Riquelme (2017), ¿Cuáles son las regulaciones del bitcoin en el mundo?

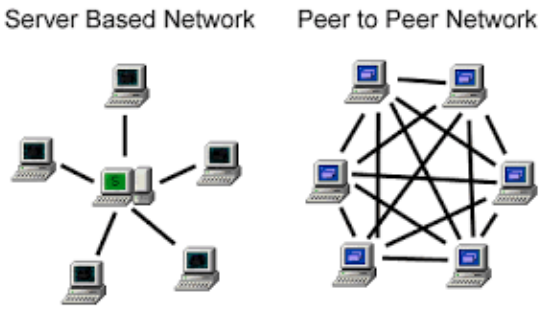
Sofía E. Mantilla. Instituto de Estrategia Nacional (2014). Bitcoin: la otra cara de la moneda.

Stephanie Lo and J. Christina Wang (2014). Bitcoin as Money?.

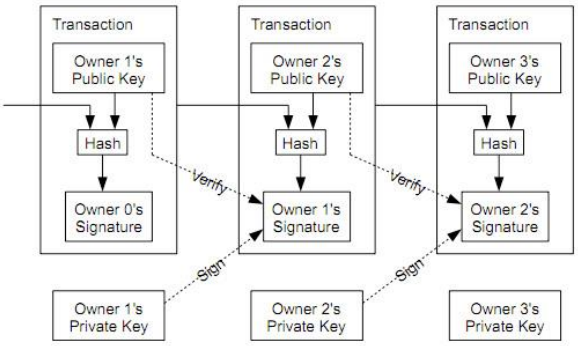
The Bitcoin Foundation . The Bitcoin Foundation manifesto.

12. ANEXOS

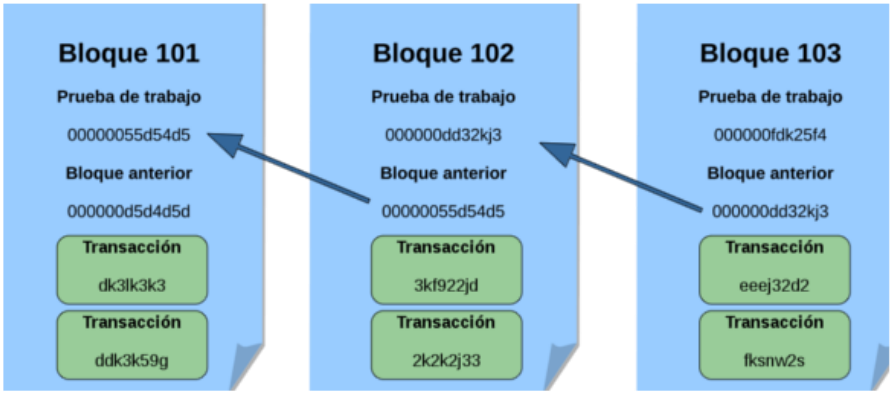
1. Red *peer to peer* (p2p)



2. *Blockchain*



3. Prueba de trabajo



Un bloque que se ha añadido recientemente a la cadena. En la parte de arriba se aprecia el número de transacciones, número de Bitcoins que se han intercambiado en este bloque concreto, y más información relevante, como el Hash, quién lo ha resuelto, cuanto pesa, etc.

En la parte de abajo se recogen las transacciones, que como se observa se realizan entre direcciones de carteras electrónicas, sin nombres ni apellidos.

Bloques #526764

Resumen	
Número de Transacciones	3186
Total de productos	3,988.58499021 BTC
Volumen Estimado de la Transacción	299.49105808 BTC
Comisiones de la Transacción	0.1021435 BTC
Altura	526764 (Cadena principal)
Fecha y Hora	2018-06-09 19:31:22
Hora de Recepción	2018-06-09 19:31:22
Resuelto por	F2Pool
Dificultad	4,940,704,885,521.83
Bits	389609537
tamaño	1179.774 kB
Peso	3997.878 kWU
Versión	0x20000000
Mientras tanto	2185080867
Recompensa del Bloque	12.5 BTC

Hashes	
Hash	000000000000000000006212efb0ad8fc5b684d3763d931213fa25468d4887e5a
Bloque Anterior	00000000000000000097f43897eb97cf812a765744d45753ae5102e9de59e9a
Bloque(s) siguiente(s)	
Raíz de Merkle	a3be2d78cf724dbafe86d978f6775aab90bea024c8a216cabc7eb4c29f8f44ce

Actas

6973acc1bde480fced3df65056597a99ec62533d4e46c78755912d88b9f1e699			2018-06-09 19:31:22
No hay entradas (monedas recién generadas)	➡	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY No se puede decodificar la dirección de salida	12.6021435 BTC 0 BTC 12.6021435 BTC

58bca14e713b8501acec3ac1d5bf89caae2dc888f9bac8e19fe7f03f811b00bb			2018-06-09 19:27:28
1FLDCfr9iG7n6bAdGsqBXmhaLgC4aSze72	➡	19NrvgnUR6FYB5wPxCHEbtbYRAKtEZuvmY	0.0010543 BTC 0.0010543 BTC

39681c426e2b967c9afb178a8c80728da3d055e419e72405e907ae4259988ed2			2018-06-09 19:27:49
1BCYpzZAmH3pX7EXU6s4gxtG1AoVMn2NfJ	➡	1D5Cx1U23CWJ6mHRoPA6UjuU2YbyRoc6x	0.0010543 BTC 0.0010543 BTC