FACULTAD DE CIENCIAS ECONÓMICAS EMPRESARIALES

TITULO:

El devenir de Bitcoin.

Aspectos y consideraciones a tener en cuenta en lo que a su futuro se refiere.

TRABAJO FIN DE GRADO

Autor: María Díaz de Bustamante Quijano

Director: Carlos Bellón Núñez-Mera

Madrid

Abril 2018

NOMBRE: María Díaz de Bustamante Quijano

TITULO: El devenir de Bitcoin. Aspectos y consideraciones a tener en cuenta en lo que a su futuro se refiere.

INDICE

*(Bibliografía al final de documento al tratarse de "Notas al Final del Documento")

INDICE DE INFOGRAPHICS, GRÁFICOS Y TABLAS

Resumen

Este informe estudia los conceptos básicos de funcionamiento de Blockchain y Bitcoin necesarios para que el lector pueda realizar un juicio justo a la hora de concebir el futuro de estas tecnologías. Además, dentro de este se va respondiendo a preguntas socialmente comunes que ponen en evidencia la falta de conocimiento de la sociedad. Como contribución de los debates planteados durante el informe, se ofrece una entrevista personal con un experto en el campo junto con gráficos explicativos apoyando los argumentos.

Palabras Clave: Bitcoin, Blockchain, Peer-to-Peer, cadena de bloques, regulación, minería, burbuja especulativa, trazabilidad, monederos virtuales.

Abstract

This paper analyses the necessary and operation concepts needed in order to make a fair judgment when it comes to conceive the future of Blockchain and Bitcoin. In addition, the typical questions asked by the society will be answered showing the lack of knowledge about these new technologies given its embryonic phase. As a contribution to the debates raised during this report, a personal interview with an expert in this sector is included along with explanatory graphs supporting the arguments.

Key Words: Bitcoin, Blockchain, Peer-to-Peer, chain of blocks, regulation, mining, speculative bubble, traceability, virtual wallets.

Introducción

Objetivos

Uno de los principales problemas a la hora de tratar con el tema de las criptomonedas, es la falta de conocimiento sobre ellas. La alta especulación de los últimos años ha producido que este activo sea únicamente visto como tal, como un activo especulativo, en vez de ser considerado por la tecnología que implica las futuras repercusiones que puede tener en las relaciones tanto en el ámbito financiero, como laboral o incluso social estas divisas digitales y cadena de bloques. Es por esto que en este informe tratará de ir respondiendo a las preguntas clave que podría hacer cualquier agente económico con el único fin de que este último se vea capacitado de poder realizar un juicio personal sobre el futuro que le ve a esta tecnología.

Metodología

Teniendo en cuenta que tanto Blockchain como Bitcoin se encuentra en unos momentos muy incipientes, a la hora de realizar los estudios pertinentes de este informe, se ha hecho uso principalmente de revistas virtuales y páginas web de monederos digitales para la recaudación de información necesaria. Es por esto que dada nuestra falta de apoyo en informes académicos, tras una búsqueda, tuvimos el placer de realizar una entrevista personal a Iñigo Molero Manglano, co-autor del libro "Blockchain: La revolución Industrial de Internet". Iñigo es un gran fanático de esta tecnología y sirvió de gran ayuda para el entendimiento de conceptos complejos junto con el análisis de algunos de los debates que se van a exponer en el informe.

Estado de la cuestión

Tras la crisis económica mundial, la sociedad pierde la confianza en los sistemas financieros tradicionales. Es entonces cuando aparece Blockchain junto con Bitcoin permitiendo así la desbancarización de los agentes económicos dada su condición distribuida junto con la optimización de modelos de negocio. Sin embargo el desconocimiento de esta tecnología impide que se evolucione y lo convierte en algo puramente especulativo.

Partes Principales del TFG

Es por esto por lo que el informe que se va a exponer a continuación consta dos grandes bloques que a su vez se dividen en 5 sub-apartados. En el primer bloque del informe se va a exponer conceptos básicos de este mundo que es Blockchain y Bitcoin, procediendo así a su explicación y ayudando al lector a entender esta tecnología.
Seguidamente el segundo bloque tratará las distintas posturas de los debates más polémicos sobre estas criptomonedas y sus posibles funcionalidades.

Hemos visto conveniente citar una parte de la entrevista con Iñigo Molero para introducir al lector en el informe, puesto que expresa muy claramente el objetivo que se va a perseguir en el estudio.

> *"Se están rompiendo muchos paradigmas. Para entender bien bitcoin, hay que desaprender muchas cosas que tenemos inculcadas desde pequeños. Yo cuando hablaba con amigos míos que eran economistas, siempre tenía el mismo problema con ellos. No lo veían, y me preguntaban, pero ¿Esto quién lo fabrica?, ¿De quién depende?, yo encantado les contestaba, "De nadie", "De todos, eso es lo maravilloso", Entonces se revolvían y me decían "Pero no hay ningún Banco central que lo respalde" y al contestarles yo que no inmediatamente me respondían "Eso es una mierda!". Se fijaban únicamente en lo que se les había enseñado, por lo que para ellos no podía existir un modelo descentralizado que optimice muchos procedimientos. Pero si eres capaz de verlo y de entenderlo, se te abre un mundo impresionante de posibilidades."* (Molero 2018)

DESCRIPCIÓN DE CONCEPTOS GENERALES

Tal y como ya se ha expuesto en la introducción, gracias a la aparición de internet y posteriormente los Smartphone y demás dispositivos electrónicos conectados a la red, existe una preocupación generalizada sobre el tratamiento de nuestros datos. Tanto la seguridad y privacidad de nuestros datos bancarios y de los movimientos se ven expuestos a terceros, instituciones bancarias y/o gubernamentales puestos a merced de comercialización, hurtos, etc.

Como respuesta a esta demanda generalizada de digitalización del sistema financiero, surge la aparición de nuevas herramientas tecnológicas que alteran el mundo financiero tanto público como privado, mejorando así su eficiencia y haciéndolo más accesible para el cliente. Entre estas herramientas se encuentran Blockchain y Bitcoin.
(Puschmann 2017)

A causa de la crisis económica mundial que tuvo su comienzo en el 2008, en la sociedad existe un sentimiento de desconfianza hacia el sistema financiero que provoca la demanda de una reforma del sistema o bien de la aparición de nuevas herramientas.

La penetración de la tecnología en la banca, puede provocar la obsolescencia de los modelos de negocio tanto de los bancos como de cualquier empresa perteneciente a cualquier sector de la industria.

Blockchain responde a esta demanda generalizada de un trato de nuestros datos seguros, de forma que los usuarios son los propios dueños y tiene el control de la red. Con esta nueva cadena descentralizada y distribuida, se ofrece una nueva perspectiva del sistema financiero, desligando así a la sociedad de las instituciones financieras de las cuales la dependencia hasta entonces había sido completa.
Se está dando un escenario donde empieza a haber tecnologías disruptivas y sobretodo Blockchain puede ser la piedra angular para optimizar esas tecnologías disruptivas y juntarlas en cierta forma para poder optimizarlas. (Molero 2018)

Tal y como iremos exponiendo a medida que avanzamos en el informe, Blockchain y Bitcoin ofrecen un método de pago completamente seguro, anónimo y desligado de cualquier gobierno o institución financiera.

BLOCKCHAIN

En 2009, tras el comienzo de la crisis económica mundial, surge el lanzamiento de Blockchain, una nueva tecnología que rompe con el método convencional centralizado a través del cual se realizan cualquiera de las transacciones financieras.

Fue un individuo o grupo que se hace denominar Satoshi Nakamoto, el creador de esta nueva base de datos, habiendo pertenecido anteriormente al movimiento CypherPunk. En 2008 Nakamoto habló por primera vez en un artículo titulado "A Peer to Peer Electronic Cash System" (Nakamoto 2008) de este nuevo método que a través de protocolos no necesita de intermediarios financieros. Lo más interesante es que Nakamoto no fue el que inventó esta tecnología, sino que lo único que hizo fue coger ideas de mentes brillantes de los últimos 40 años (La teoría de las claves públicas, el sistema Peer to Peer, etc. [1]) y juntarlas en esta nueva tecnología, la cual denominaría más tarde Blockchain y Bitcoin.

Blockchain transforma todos los convencionalismos de las transacciones que se habían hecho hasta la fecha, cambiando la forma tanto de vender como de comprar cualquier tipo de activo siendo estos tanto financieros como de cualquier tipo de valor, junto con la forma de interactuar entre ambas partes de la transacción.

¿Qué es Blockchain?

Se trata de una **base de datos** completamente distribuida organizada en bloques de información repartidos entre los diferentes participantes de la cadena, donde todas las transacciones realizadas son grabadas de forma irrevocable en la cadena de bloques.

[1] En el caso del que el lector quiera saber más sobre estas teorías puede visitar las siguientes direcciones:
- https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida
- https://www.ecured.cu/Red_Peer_to_Peer

Este método de interacción entre ordenadores utilizado por Blockchain es denominado *"Peer-to-Peer"* (**P2P**) o "*Red entre pares*". (Smith 2017)

P2P es una red de ordenadores interconectados entre sí en la cual todos los participantes, en este caso llamados "nodos", actúan en la red de forma simultánea como servidores y clientes permitiendo intercambios de información entre ellos. Todos los usuarios tienen la misma condición, ninguno se encuentra en un nivel jerárquico superior a otro, por lo que son todos semejantes entre sí. (Bima 2017)

La condición de base de datos **distribuida** indica que todos los nodos que forman parte de la red como almacenamiento de los bloques de información, no están ligados a un ente centralizado, sino que cada que cada cadena de bloques tiene el control y el derecho de modificar dichos bloques bajo consenso de todos los usuarios, sin tener que responder ante una misma institución. (Rosic 2017)

Tal y cómo nos contaba Iñigo Molero en la entrevista que tuvimos el placer de tener con él:

> *"Blockchain es el internet del valor […] Si yo te mando una foto ese archivo se replica. Pues Blockchain lo que consigue es que […] podamos transmitir valor a través de internet […] Es una tecnología que ha llegado para quedarse, y que ahora mismo estamos en unos momentos muy incipientes"* (Molero 2018)

¿De qué se compone un bloque de Blockchain?

En términos generales, un bloque de Blockchain contiene la información de todas las transacciones que forman dicho bloque. Existen tres conjuntos fundamentales de información en cada bloque (Lewis 2015):

- En primer lugar, los **datos fundamentales de las transacciones.** En el caso de una transacción de Bitcoin, estaríamos hablando del monto de la transacción y de la identidad (en forma de pseudónimo como veremos más adelante) de todas las partes implicadas en estas.
- En segundo lugar, **cada bloque tiene un Hash**. Un hash es como una huella de identidad única para cada bloque de la cadena que es calculado

por los mineros (de esto consta el proceso de minería que se detallará en próximas partes del informe). Si algún componente del bloque es modificado (siempre bajo consenso de todos los nodos), el hash cambia. Esto es muy útil a la hora de darse cuenta de si ha habido algún cambio en los bloques.

- Finalmente, **cada bloque contiene el hash del bloque anterior.** Esto provoca una interconexión entre los bloques, por lo que es prácticamente imposible un intento de hackear o modificar un bloque sin el consentimiento de la red, dado que implicaría tener que engañar a todos los nodos y crear una cadena mayor que la verdadera (este concepto se explicará más adelante). El primer bloque creado se denomina "Bloque Génesis" y es el único de la cadena que no contiene el hash del bloque anterior puesto que no existe uno anterior a él.

Dado el poder de computo de los ordenadores de hoy en día, cualquier ordenador podría crear miles de hash cada minuto por lo que se producirían millones de bloques nuevos al día. Es por ello que Blockchain utiliza el sistema "Proof of Work" que ralentiza el proceso de creación de los bloques.

Proof of Work

Proof of Work (con abreviatura POW) es un sistema de prueba interactiva costosa (tanto de tiempo como de dinero) por el cual, los mineros deben de descifrar un enigma con el fin de ser los primeros en conseguir crear el hash y que de esta forma los nodos puedan validarlo posteriormente, provocando así la creación del nuevo bloque y recibiendo por ello una retribución económica. En el caso de minería de Bitcoins, la resolución/creación del hash y por lo tanto la validez del nuevo bloque de transacciones es recompensada con estas criptomonedas, siendo el monto de la recompensa la cotización de ese momento de los bitcoins junto con las comisiones de las transacciones. (Bulkin 2016)

Del mismo modo, con el Proof of Work se garantiza la seguridad de la cadena de bloques. Gracias a la criptografía que resulta de la resolución de estos problemas, se previene la entrada de hackers o cualquier otro agente externo que quiera realizar

fraudes. Tal y como se ha mencionado anteriormente, se necesita de la aprobación de toda la cadena para la creación de un nuevo bloque. Esto supone que toda la cadena forma parte de cada una de las creaciones de bloques. En el caso de que se quiera "falsificar un bloque" sería necesario tener el control de más de la mitad del poder de cómputo, es decir del 51% de los nodos, para que de esta forma los bloques fraudulentos sean verificados y pasen a formar parte de la cadena. (Sánchez de Diego 2014)

Con el POW se garantiza que el trabajo realizado es el correcto y ha consumido tanto el tiempo como el dinero de los mineros el hecho de resolverlo. Gracias a la dificultad de los problemas matemáticos criptográficos, se ralentiza la creación de bloques como ya veremos más adelante.

En el caso de Bitcoin como se explicará en la segunda parte del informe el sistema de POW utilizado es el HashCash.

¿Cómo funciona Blockchain?

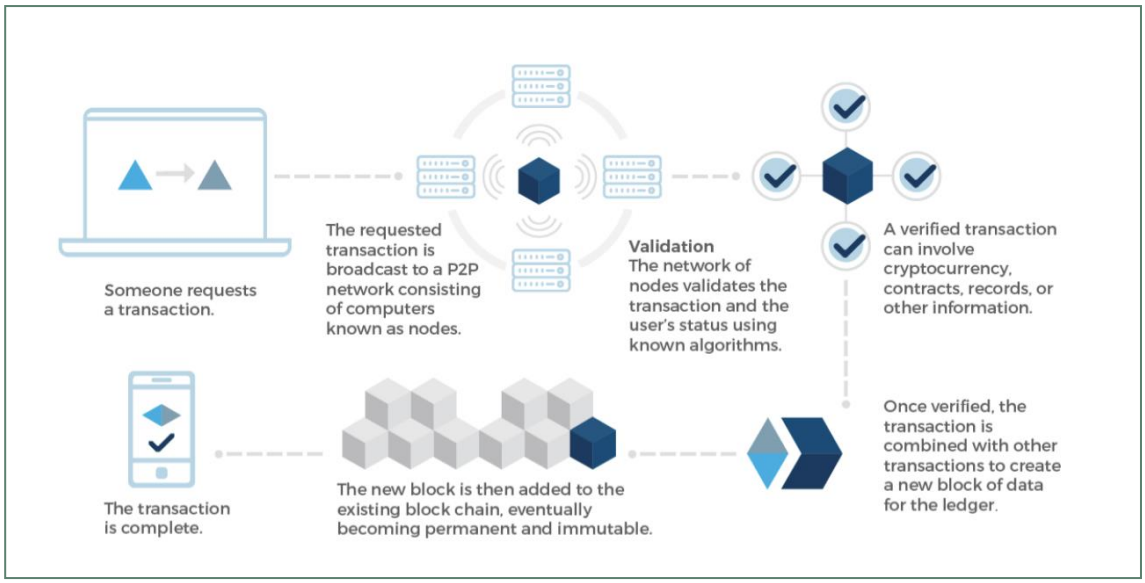
Como se ha expresado anteriormente, Blockchain es una base de datos distribuida, en la que todas las transacciones realizadas son grabadas en la cadena de bloques de forma irreversible e inmutable. A continuación, estudiaremos las fases de creación de bloques de Blockchain en la cual participan los mineros[i].

1. Se **solicita** realizar una transacción a través de la cadena.
2. La transacción solicitada es enviada a la red P2P compuesta por los nodos de Blockchain junto con más transacciones para **pasar a su verificación** (también llamado resolución del problema).
3. Los **mineros compiten** para verificar el bloque.
4. A través de una serie de cálculos matemáticos (POW), se **determina que las transacciones son válidas** y que cumplen con la normativa necesaria, por lo que se genera el bloque. Se necesita el consenso del 51% de los nodos para que una transacción sea verificada y tenga validez. Más adelante en el informe se estudiará qué pasa con las transacciones que no han sido verificadas y el proceso mediante el cual se incluyen en los bloques.

5. **El hash hallado por los mineros es incluido en el bloque** pasando a ser este su "sello de identidad" a no ser que su contenido sea modificado posteriormente. Gracias a este hash, **el bloque pasa a formar parte de la cadena** y tal que como se ha expuesto en apartados anteriores no se puede falsear. [ii]
6. Finalmente **se realiza la transacción creándose una especie de contrato inteligente por la red** que gestiona y controla de forma directa la transacción que se está llevando a cabo de activos digitales. La unidad de valor es intercambiada entre las partes. Dicha unidad de valor no tiene por qué ser monetaria, sino que también puede tratarse de otros activos como un título de propiedad, un título educativo, etc.

Este proceso lo podemos ver ilustrado para su mejor comprensión en el diagrama expuesto a continuación publicado por la página Web Blockchain en el WhitePaper.

Infographic 1 : Funcionamiento de Blockchain



Fuente: Infographic extraído de la página web de Blockchain siendo este un Wallet[iii]

Podemos apreciar que cualquier movimiento realizado en Blockchain queda grabado irreversiblemente en un bloque puesto que éste pasa a formar parte de la cadena, sin poder modificarse salvo consenso de todos los participantes de que el cambio deseado es verídico (esto pasa pocas veces dado que como se ha mencionado antes, debe de ser consenso del 51% del poder de computo de la cadena).

Cada cadena de bloques tiene un protocolo común para todas las personas implicadas en esta. Todos los participantes deben recibir una copia actualizada y completa de todas las operaciones realizadas en la cadena.

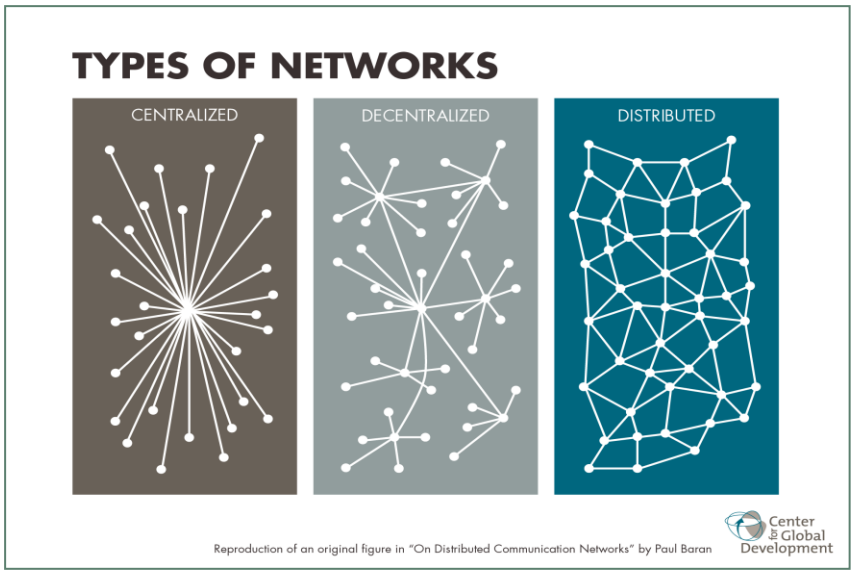
Podemos decir que Blockchain **cambia por completo todos los convencionalismos de cómo compramos y vendemos activos, la forma de interacción entre los partícipes de una transacción y la relación de estos ingresos y gastos económicos con los Estados y Gobiernos dada su descentralización. Esta descentralización se debe a una desaparición de la necesidad de un registro central, al igual que la oportunidad de realizar un traspaso de activos financieros de forma completamente digital.**

¿Qué caracteriza a Blockchain?

Blockchain tiene una serie de características que la hacen única convirtiendo a esta red como la propulsora de métodos de pago descentralizados, eficientes y sin intermediarios financieros[iv].

- En primer lugar, la **rapidez**. La desintermediación de las transacciones gracias al P2P utilizado, hace de esta cadena de bloques un sistema para realizar transacciones bastante rápida. No es necesaria toda la burocracia de las instituciones financieras para confirmar las transacciones. De media, cada 10 minutos un bloque es creado, por lo que todas las transacciones incluidas en ese bloque han tomado lugar y han sido finalizadas. Mientras que hacer una transferencia bancaria a Estados Unidos por ejemplo puede llegar a tardar 1 semana, haciendo uso de la tecnología de Blockchain, este proceso puede llevarse a cabo en 10 minutos. En la siguiente imagen podemos apreciar de forma esquematizada la diferencia entre una red centralizada, descentralizada y distribuida, siendo ésta ultima la que utiliza Blockchain. No existe un núcleo o ente centralizado que controle el resto, sino que, al estar formada por cadenas de bloques interconectados, esto permite que la red está completamente distribuida. Por lo tanto, cada uno de los nodos de la red participan en la gestión y deben de autorizar cualquier transacción realizada en esta.

Infographic 2 : Condición de red distribuida de Blockchain



Fuente: "Blockchain and Economic Development: Hype Vs. Reality" (Pisa 2017)

Todos los dispositivos que forman parte de la cadena de bloques (pueden ser desde un ordenador particular hasta uno de alto rendimiento) controlan toda la información de Blockchain, de ahí que se denomine "cadena", ninguno de los nodos se ve excluido de la toma de decisión. Esto es opuesto a las redes centralizadas del sistema financiero donde es una única entidad la que controla y recauda todo para luego distribuirlo.

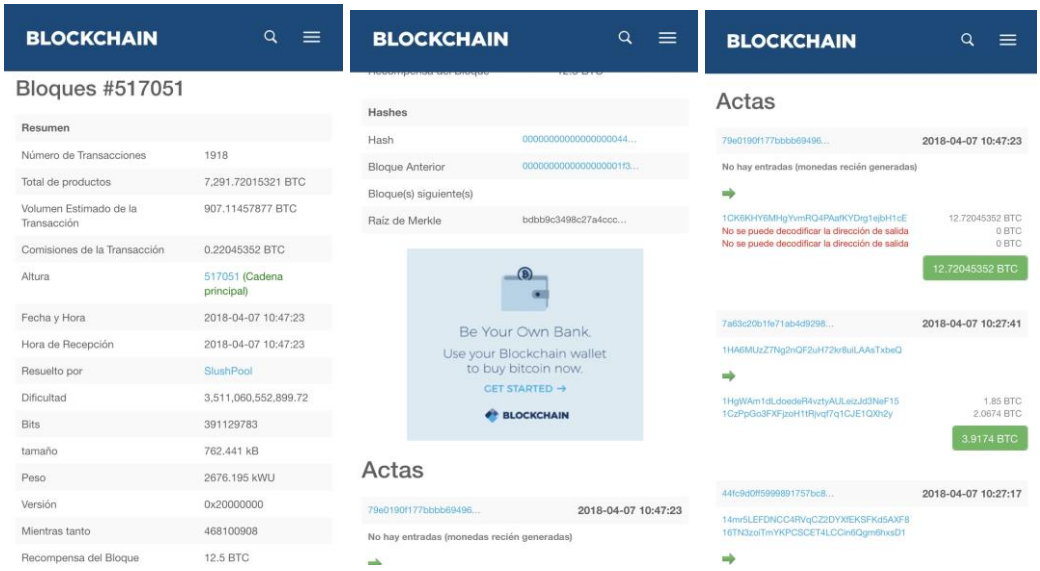
- Por otra parte, la **transparencia que resulta en seguridad**. Todas las transacciones realizadas en Blockchain, son completamente públicas y accesibles a cualquiera. Sin embargo, a pesar de que cualquier persona puede ver las transacciones que se han realizado hoy mismo en la cadena, estas están bajo forma pseudo anónima, por lo que la identidad de los participantes queda salvaguardada. Esta transparencia provoca un sentimiento de seguridad puesto que toda la información correspondiente de las transacciones es completamente pública y está a disposición de cualquiera, nada es ocultado.

  A pesar de ello, como se estudiará en el siguiente apartado, existen ciertos tipos de Blockchain que no cumplen íntegramente esta condición de transparencia.

  En las siguientes tres imágenes, podemos apreciar que en la página web Blockchain.info, se pueden observar todos los bloques creados, junto con toda la información de la que se componen estos y todas las transacciones que han sido

incluidas en los bloques. La fácil accesibilidad de esta información en una página web pública muestra la transparencia de esta cadena de bloques.

Infographic 3: Capturas de Pantalla de un bloque de la cadena Blockchain



Fuente: Página Web Blockchain.info[v]

- **Blockchain ofrece seguridad en toda su esencia.** Gracias a la utilización de Hash, el sistema no puede ser falseado, dado que como se ha expuesto anteriormente, en caso de que se cambiase algo en un bloque, el hash cambiaría y la cadena quedaría descuadrada por lo que todos los participantes se darían cuenta. Del mismo modo, la criptografía también favorece la seguridad ofrecida por esta cadena de bloques. Gracias a una serie de algoritmos con accesibilidad a través de clave, toda la información tratada por Blockchain es indescifrable para cualquier individuo que no tenga en su pertenencia esas claves. Esta criptografía también evita tanto el fraude como el hurto. Es gracias a todas estas medidas por lo que el usuario que está participando en la red se siente seguro (Naranjo 2017).

Cabe destacar que no existe únicamente una Blockchain, sino que se han ido creando otras modalidades que principalmente cumplen las características aquí mencionadas, pero no todas de la misma forma. Cada derivado de la Blockchain original (Blockchain de Bitcoin) puede tener distintas características y tratar distintos tipos de activos, no tienen que ser específicamente criptomonedas, sino que como se ha mencionado anteriormente nos encontramos ante una red de intercambio de valor mediante la cual se puede hacer intercambio de cualquier activo con algo de valor. Dentro de las

modalidades existen dos principales, la Pública y la Privada, de las cuales derivan luego el resto. Es por ello que siendo estas las bases de todas las Blockchain existentes, que vamos a proceder a su análisis.

Blockchain pública Vs. Blockchain Privada

La principal diferencia entre ambas modalidades es principalmente el nivel de accesibilidad que tiene la red, como está de limitado su acceso. Asimismo, como veremos a continuación, los niveles de transparencia van a ser dispares[vi].

- Blockchain Pública

Esta Blockchain pública o también llamada "sin permisos" fue la que apareció en 2009 junto con Bitcoin, siendo esta la que de forma general se ha ido definiendo en los apartados anteriores. Es considerada la modalidad más característica y conocida de ambas dado que va de la mano con la condición de transparencia que define a Blockchain (Jayachandran 2017).

Entre las principales características de la Blockchain Pública podemos encontrar:

- Se trata de una red **pública**, cualquier persona, sea esta usuario o no de la red, puede acceder y ver las transacciones y movimientos realizados en ella.

- Es una red **abierta**, es decir que cualquier individuo puede convertirse en participante de la cadena, no existe ningún tipo de requisito. (Bima 2017)

- Se trata de una red **distribuida pseudo anónima**. Por un lado, todos los nodos están en el mismo nivel jerárquico, es decir que ninguno tiene más poder que el otro, y las identidades son irreconocibles personalmente. Todas las transacciones se producen bajo un pseudónimo, en ningún momento está explicito el nombre de la persona que realiza la operación.

- Blockchain Privada

Esta modalidad de Blockchain, a diferencia de la pública aparece más tarde, en el 2015 ante la demanda de las instituciones financieras y otras organizaciones de querer participar en la red (Bima 2017).

Este tipo de organizaciones que quieren invertir en esta tecnología, pero se ven limitadas dado que se ven sometidas a ordenes regulatorias y de confidencialidad, no se pueden permitir el hecho de que sus datos se vean expuestos públicamente.

- Las principales diferencias que tiene Blockchain Pública con Blockchain Privada son como bien dice su nombre la condición de **privacidad.** La información de la que están compuestos los bloques no es accesible para cualquier particular, sino que sólo algunos de los usuarios pueden acceder a la información de algunas de las transacciones. Es por esto por lo que esta modalidad de Blockchain también se denomina "Blockchain con permiso".

- Del mismo modo, esta condición de privacidad afecta al acceso a la red. No cualquier persona puede llegar a formar parte de la cadena y adquirir esta condición de usuario. Con lo cual, la Blockchain Privada se puede considerar una red cerrada.

- Finalmente, Blockchain Privada se caracteriza por tener un **control interno** en vez de externo. En la red privada son los usuarios internos los que se comprometen a gestionar la estabilidad del sistema, por lo que la condición de "distribuida" no está del todo presente en este tipo de Blockchain.

Un claro ejemplo de una Blockchain Privada es Alastria de la cual Comillas es miembro fundador. Esta cadena de bloques permite la interacción entre instituciones tanto públicas como privadas españolas cumpliendo con la idea de que esta cadena de bloques cumpla con la regulación del estado, de ahí que se haya elegido la categoría de privada para esta Blockchain. Dentro de esta Alastria se produjo un pago por energía entre Gas Natural y Endesa[2].

[2] En caso de interés, visitar la página web alastria.io

Adicionalmente, en otros aspectos ambas modalidades se siguen pareciendo. La inmutabilidad de los datos de los bloques sigue siendo la misma, al igual que son inalterables.

De igual forma, no es necesario el uso de una de estas modalidades en su integridad, sino que se pueden hacer híbridos entre ambas cambiando características de estas siempre y cuando sea posible. Este sería el caso de una Blockchain con una gestión de los usuarios identificados pero que sin embargo tiene una visibilidad pública.

Transparencia de la propiedad.

Es sujeto de estudio la condición de transparencia anteriormente nombrada de las cadenas de Blockchain puesto que es uno de los aspectos innovadores y que caracteriza a esta nueva plataforma de transacciones y tratamiento de datos. Esta característica de la cadena ya se ha puesto en evidencia anteriormente en el informe junto con la explicación de la seguridad de Blockchain).

La principal razón por la que se habla de transparencia es que, tal y como se ha mencionado anteriormente, una copia de todas las transacciones realizadas en la cadena de bloques es distribuida de forma completamente transparente y visible a todos los participantes, esto ayuda a la condición de "red distribuida" de Blockchain. Una empresa que participa en una Blockchain Pública, se va a ver beneficiada por este tipo de distribución dado que todos los accionistas y otras partes interesadas van a ser capaces de ver los movimientos realizados con los títulos de propiedad de la empresa a la misma vez que van a ser avisados de cualquier cambio realizados en estos, dentro siempre de los límites impuestos por la condición pseudo anónima de la cadena. (Smith 2017)

Sin embargo, no todos los agentes financieros se van a ver atraídos por esta transparencia. Mientras que unos agentes buscan ser transparentes en cuanto a sus movimientos se refiere, otros van a ser perjudicados dado que no están interesados en que sus transacciones sean "abiertas" puesto que lo que quieren es encubrirlas.

Tras este estudio del funcionamiento y componentes de la cadena de bloques Blockchain, vamos a proseguir con un análisis de Bitcoin teniendo en cuenta que el

propósito de este informe es el de analizar cuál va a ser el futuro de esta criptomoneda y si de verdad se considera un activo perpetuo.

BITCOIN, LA PRIMERA CRIPTOMONEDA.

Bitcoin fue la primera moneda virtual descentralizada, que no está respaldada por ningún gobierno o economía siendo impulsada por sus propios usuarios. Esta criptomoneda es una red consensuada en la cual se permite realizar pagos con la moneda virtual denominada "token" o "bitcoin", de una forma pseudo anónima y segura, sin intermediarios realizando las transacciones entre el ordenante y el beneficiario. (Bima 2017)

Bitcoin aparece por primera vez en 2009 junto con Blockchain de la mano de su creador Satoshi Nakamoto, hoy por hoy sigue siendo desconocida la verdadera identidad y procedencia de este. Esta criptomoneda introduce en el mercado un nuevo sistema de pago que permite de forma pseudo anónima realizar pago de transacciones por cualquier valor haciendo uso de los bitcoins como moneda de cambio y de la cadena de bloques de Blockchain como plataforma para las transacciones.

Tras su lanzamiento, este tipo de moneda virtual descentralizada causaba mucha intriga y confusión dada su compleja tecnología y que no tiene un valor intrínseco en sí. Es por esto que, durante su primer año de vida, el valor de Bitcoin no llegó si quiera a un dólar puesto que no estaba respaldada por ningún gobierno ni activo y los agentes no entendían bien cual podía ser su utilidad.

Hoy en día, no nos es de extrañar escuchar preguntas del tipo *¿Qué es un Bitcoin? ¿Para qué sirve exactamente? ¿Qué usos se le puede dar? ¿Dónde se pueden encontrar?*

Tal como se ha expresado anteriormente, Blockchain y Bitcoin fueron los dos lanzamientos revolucionarios que cambiaron la forma de concebir las transacciones monetarias. Es por esta condición novedosa y compleja que presenta Bitcoin por lo que vamos a proceder al estudio de sus principales características y funcionamiento.

¿Cómo funciona Bitcoin?

Para poder realizar un estudio del funcionamiento de las transacciones realizadas con Bitcoin, hay que mencionar también conceptos anteriormente explicados en este informe en apartados anteriores, como la red "Peer to Peer" y Blockchain.

En términos generales tener en tu propiedad un Bitcoin, significa tener en tu posesión las claves públicas y privadas de una unidad de esta criptomoneda (cuyo valor es la cotización de cruce con divisa deseada en ese momento) con la cual se puede realizar una única transacción, es decir que se puede hacer un único uso de dicha unidad de criptodivisa[vii]. En futuros apartados, veremos cómo se puede llegar a obtener un bitcoin.

Al tratarse de una moneda virtual, no existe ningún elemento físico que garantice la propiedad de dicho activo monetario, un bitcoin no es más que una denominación criptográfica que tiene el usuario dentro de su **cartera virtual (también denominados monederos Bitcoin, Wallets, etc.)**.

Estos monederos virtuales son estrictamente necesarios a la hora de querer adquirir, almacenar o vender cualquier criptomoneda[viii], en este caso Bitcoin. Un monedero es aquel que te da acceso a la red de Bitcoin puesto que es en este dónde se van a almacenar todos los datos criptográficos, como es el caso de las claves tanto públicas como privadas, de los bitcoins que se van a poseer. Más adelante estudiaremos las diferentes modalidades de monederos virtuales que existen hoy en día.

Para la mejor comprensión y explicación de las transacciones de Bitcoin[ix], lo vamos a ilustrar con un ejemplo de elaboración propia.

- A le quiere comprar a B un libro que tiene y le encanta, por 1 bitcoin.
- B le da la clave pública de su monedero de bitcoins a A para que comience con la transacción.
- A solicita a la red que la transacción sea verificada y posteriormente escrita en un bloque, dentro de la cual ha incluido su clave pública, la clave pública de B para que las criptomonedas sean transferidas a SU monedero, el monto de la transacción, y finalmente la clave privada, siendo A la única conocedora de esta última por lo que ella es la única que puede firmar transacciones con esta moneda. La revelación de

esta última clave tiene un papel esencial en la transacción dado que va a ser la que demuestre que efectivamente A tiene en su poder la criptomoneda a entregar.

- B es informado de que se ha verificado la transacción y de que esta ha pasado a formar parte de un bloque de la cadena de Blockchain.
- Cualquier persona puede visualizar bajo la denominación de las claves públicas de A y B, que estas dos partes han realizado una transacción con bitcoins y el monto de esta.

En las siguientes capturas de pantalla sustraídas de la página web de Blockchain podemos observar un ejemplo real de transacción de Bitcoins que se ha realizado mientras se escribía este apartado (en tiempo real). Aquí podemos apreciar todos los componentes de una transacción de Bitcoin que acabamos de mencionar. En el caso del ejemplo utilizado para ilustrar las transacciones, las claves públicas de los bitcoin de A serían las ubicadas a la izquierda de la imagen, mientras que la clave pública del monedero de B sería la de la derecha. Cabe destacar el botón rojo que permite declarar que esta transacción no es válida dado que se conoce que los bitcoins intercambiados ya han sido utilizados anteriormente en otra transacción. La razón por la que existe la posibilidad de declarar este doble gasto es porque la transacción aquí mostrada no ha sido aún verificada, es decir que todavía no ha sido incluida en un bloque por lo que no forma aun parte de la cadena Blockchain.

Infographic 4: Capturas de Pantalla de Transacción sin verificar de Blockchain de Bitcoin

En Bitcoins (BTC)

Fuente: Página Web Blockchain.info [x]

En dólares ($)

Fuente: Página Web Blockchain.info

En esta transacción podemos ver las comisiones cobradas por bitcoin a la hora de realizar una transacción. En el momento en que se produjo la transacción aquí expuesta, la tarifa de comisiones por transacción es de 0.407 satoshis (Más adelante se explicará más en profundidad las comisiones de cada transacción y los satoshis). Adjuntamos a continuación por si el lector quiere comprobar la veracidad de la información expuesta, el link de la plataforma de Blockchain donde se pueden apreciar las transacciones pendientes de confirmar en tiempo real:

https://blockchain.info/unconfirmed-transactions

La facilidad de acceso a esta página web en la cual aparecen todas las transacciones realizadas en la cadena de bloques, pone en evidencia la condición de transparencia de Blockchain y por consecuente de Bitcoin anteriormente citada.

A continuación, entraremos en un análisis más explícito de los aspectos de los que se compone un bitcoin, los cuales posteriormente son incluidos en las transacciones. Hemos podido observar de las explicaciones anteriores que, en términos generales, un bitcoin se compone de tres aspectos[xi]:

- Las **claves públicas**: son aquellas que identifican a los usuarios bajo forma de seudónimo. Las claves públicas son intercambiadas entre las partes de la transacción para que estas sepan a qué usuario deben transferirle las monedas. Por o tanto la

clave pública es aquella usada para recibir los bitcoins, es decir que sirve como dirección de identidad del receptor.

- La **clave privada** la posee únicamente el propietario de la criptomoneda que va a ser transferida. Es únicamente bajo el conocimiento de esta clave que es posible el acceso a las cuentas de bitcoin y a su gasto en el momento de pago de una transacción[xii].
- Finalmente, existe la **firma digital**. Con este tipo de firma se garantiza que la persona que está realizando la transferencia de bitcoins con las claves es la auténtica dueña de esas monedas. Esto se debe a que estas firmas son elementos criptográficos que se calculan a partir de la clave privada demostrando así la propiedad del bitcoin.

Como conclusión, podemos afirmar que una transacción de Bitcoins es una transferencia de valores entre Wallets que debe ser incluida en la cadena una vez sea verificada y confirmada.

Seguridad y confidencialidad de Bitcoin.

La criptografía es el elemento fundamental que garantiza la seguridad en el momento de hacer uso de la red de bitcoin para las transacciones, de ahí que este tipo de moneda digital se denomine **"criptomoneda".**

La criptografía es el uso de una serie de protocolos y cálculos encriptados mediante los cuales es posible verificar y autentificar las transacciones realizadas. Existen una serie de cualidades que obtiene Bitcoin gracias al uso de esta encriptación.

- Por una parte, existe una **vinculación** entre la propiedad del bitcoin y el supuesto propietario gracias a las claves públicas criptográficas proporcionadas en el momento de posesión de la criptomoneda, las consecuentes direcciones públicas y privadas junto con la firma digital que son calculadas gracias a los métodos criptográficos utilizados por Bitcoin.

- Existe una **integridad** y **autenticidad** de la red gracias a la verificación y al sistema de "cadenas" de la red (como es el caso de los "hash" anteriormente estudiados en el apartado de Blockchain) por lo que la red no puede ser falseada. Gracias a esta validación de las transacciones por parte del sistema y a la interconexión entre los nodos no existe posibilidad de falsificación y de hurto de las monedas. (Sánchez de Diego 2014)

- Finalmente, gracias a la utilización de criptografía, existe un nivel de **confidencialidad**. A pesar de que la red es pública y todas las transacciones pueden ser observadas por cualquier tercero, todas las operaciones se realizan bajo claves alfanuméricas (o pseudónimos) creados por un software específico de Bitcoin. Del mismo modo, tal y como se ha expresado antes con el ejemplo de la transacción entre A y B, únicamente las claves públicas son aquellas mostradas en la red, las claves privadas sólo van a ser conocidas por el propietario original de la moneda en el momento de la transacción. Bitcoin hace uso del algoritmo ECDSA que permite "derivar de una clave privada, la clave pública correspondiente y así poder validar las firmas digitales hechas con esa clave privada" (Montes 2017).

¿Se puede hacer un doble uso de la misma moneda?

Cada bitcoin puede ser utilizado/gastado por un mismo usuario una única vez. Es gracias a la cualidad de autenticidad, por la que no es posible la **doble contabilidad o doble gasto de un bitcoin**[xiii]**.**

Un mismo usuario **no puede duplicar la moneda**[xiv] para gastársela dos veces dado que toda la información de la transacción, incluidas las claves de la moneda han sido inmediatamente enviadas para su posterior verificación a todos los participantes de la cadena. Asimismo, esta transacción ha formado parte del motivo de creación de un bloque por lo que no puede "pasar desapercibida". Podemos ver un claro ejemplo de esto en Infographic 4 que muestra un ejemplo de transacción de bitcoins, donde existe la posibilidad de denunciar un doble gasto de forma inmediata.

Por lo tanto, podemos afirmar que el sistema criptográfico de la cadena de bloques y la minería (que explicaremos más adelante) son las dos herramientas que imposibilitan el doble gasto de un bitcoin.

Haciendo uso del ejemplo de transacción anteriormente nombrado, B habiendo recibido la confirmación por parte de Blockchain de que las claves son las correctas, se asegura que el bitcoin obtenido era efectivamente de A y que la transacción es válida.
Del mismo modo A no puede intentar volver a usar el mismo bitcoin que le entregó a B, dado que las claves de esa moneda y la información de la transacción ya se encuentra en una gran parte de la cadena y gracias a que **la información de los bloques es inmutable** (Bima 2017), esta información no puede ser modificada salvo que consiga el control de la mayor parte de la red CPU del sistema (pero tal y como se ha expresado en apartados anteriores esto se considera prácticamente imposible).

Pseudo anonimato de Bitcoin

Blockchain no se considera una sistema completamente anónimo, sino que se dice que es dice que es pseudo anónimo dado que las claves públicas (seudónimos) de cada transacción son publicadas en la cadena, al igual que se le envía a todos los participantes una copia de esta[xv].

Cada saldo de monedas está matemáticamente ligado a un pseudónimo que a su vez va ligado con las claves de las criptomonedas de las que está compuesto.

Un ejemplo de una clave pública podría ser (siempre empiezan por 1 o 3):

3Pj9ayC4hNX2rmihrt7uHTgtc6fYAS3UVtvhRbpl8h4UN

Cada usuario puede tener varias claves públicas (pseudónimos), y cada una con distintos montos, de tal forma que se dificulta que su identidad sea deducida, aumentando así el nivel de privacidad. Del mismo modo, el propietario siempre tiene derecho a cambiar de motu propio las claves públicas y privadas de las criptomonedas que tiene en su poder para estar así más seguro. (Montes 2017)

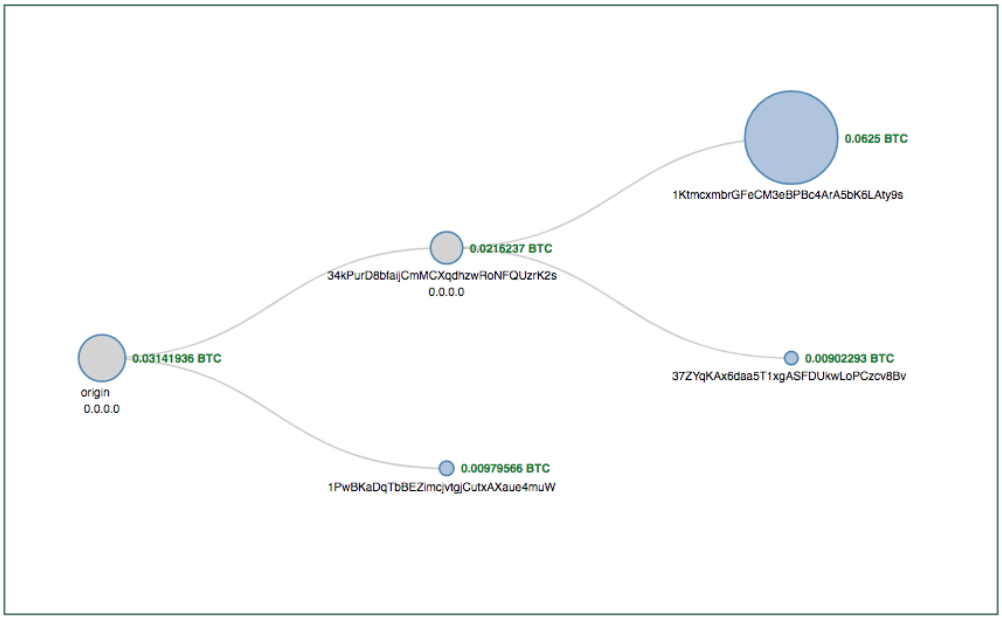
Problemas de trazabilidad

A pesar de todas estas medidas, existen instituciones que se dedican a la identificación de los usuarios que realizan las transacciones. Estas organizaciones gracias a la información otorgada por Blockchain, pueden deducir la identidad de los

usuarios de la red a causa de su trazabilidad. La propia plataforma de Blockchain ofrece la posibilidad de visualizar un Árbol de Merkle y de esta forma ver todo el recorrido que han tenido las criptomonedas. (Birma 2017) En la siguiente imagen podemos apreciar uno de los arboles disponibles en la página web de una de las transacciones del bloque mostrado en apartados anteriores producidas mientras se escribía este párrafo.

ChainAnalysis es un claro ejemplo de empresa que busca identificar los usuarios de esta cadena de bloques. Su lema es "Prevenir, Detectar e investigar el lavado de criptomonedas, fraude e incumplimientos de la ley"[xvi].

Infographic 5 : Árbol de Merkle de una transacción de Blockchain



Fuente: Página Web Oficial de Blockchain [3]

¿Cómo adquirir un Bitcoin?

A la hora de estudiar cómo se puede obtener un bitcoin, existen tres formas generales: Minando un bloque, adquiriéndolo en un Exchange y finalmente en una ICO (Initial Coin Offering).

[3] https://blockchain.info/es/tree/340600246

- Minería de Bitcoin

El sistema por el cual se mina un bitcoin, es el estudiado anteriormente en este informe junto con Blockchain y Proof of Work (POW). En el momento en el que una transacción solicita ser validada por la red y pase a formar parte de la cadena y tome lugar el intercambio, se les da un aviso a los mineros para que se inicie le proceso de minería. (Sánchez de Diego 2014)

Tal y como se explicó anteriormente, el POW es el sistema por el cual a través de resolución de problemas matemáticos con un poder de computo suficiente para poder estar trabajando 24 horas, los mineros son capaces de verificar un bloque de la cadena de Blockchain. Gracias a esta verificación, el bloque es creado por lo que las transacciones que han sido verificadas, siendo estas las que se desea incluir en un bloque, pasan a formar parte de la cadena. Está demostrado que en el caso de bitcoins, cada 10 minutos un bloque nuevo es creado, por lo que cada 10 minutos un minero es recompensado dado que ha conseguido "resolver el problema" antes que los demás mineros que compiten contra él. (Nakamoto 2008)

Únicamente aquel minero que haya conseguido verificar el bloque, recibe una recompensa monetaria que en este caso estaría compuesta por bitcoins. El monto de la recompensa obtenida variará dependiendo del valor al que coticen los bitcoins en ese momento. Cabe destacar que el proceso de minería no resulta gratuito para los participantes, puesto que el poder de cómputo continuo necesario para la minería es muy costoso, a la misma vez que requiere mucho tiempo de trabajo.

Además de la utilización del sistema POW utilizado por Blockchain y Bitcoin, Satoshi Nakamoto impuso dos condiciones que limitan la velocidad de creación de los bloques, por lo tanto de la minería, y que convierten a esta criptomoneda en un bien preciado y escaso:

- Únicamente existirán 21 millones de Bitcoins, ni uno más, ni uno menos. Este número finito de bitcoins provoca que la demanda de estas criptomonedas sea por norma general superior a la oferta disponible. Es por ello que, ante el aumento de la demanda de este "tipo de moneda de cambio", en los últimos años se ha producido

el lanzamiento de más de 1.500 criptomonedas alternativas (también denominadas altcoins). Sin embargo, por el momento bitcoin sigue siendo la más influyente y la que más volumen de mercado tiene. Esto puede deberse a su antigüedad o a su condición de "primera criptomoneda de la historia". (Nakamoto 2008)

Dada la falta de condición física de los bitcoins, un bitcoin podría ser fraccionado de forma infinita lo que invalidaría el límite de oferta de 21 millones que fue impuesto, pudiendo haber infinitos bitcoin si los fraccionamos todas las veces que queramos. Es por esto por lo que Satoshi Nakamoto cuando creó Bitcoin, indico que lo máximo que se podría fraccionar una unidad de esta criptomoneda fuese en "un satoshi" (100.000.000 = 1 Bitcoin) limitando así la oferta y la cantidad de uso de bitcoins en el mercado.

- Está estipulado dentro de los fundamentos de Bitcoin, que cada cuatro años se reduce a la mitad la cantidad de tokens que reciben los mineros por la verificación de cada bloque. Este fenómeno se denomina "halving"[xvii]. A partir de 2016 (la última reducción), un minero recibe 12,5 BTC + comisiones de transacción (c.t.) por cada bloque creado, a diferencia de 2012 donde se recibían 25 BTC + c.t. y 2009 donde se recibían 50 BTC + c.t. Las comisiones de transacción, no se ven afectadas por esta reducción. Esta disminución seguirá llevándose a cabo hasta alcanzar la cantidad finita de 21 millones de bitcoins. En el momento de redacción de este apartado habían minados únicamente 16.954.463 bitcoins.

  Las comisiones de transacción son por llamarlo de alguna forma, el "pago" que le hacen los usuarios a los mineros por incluir sus transacciones en un bloque. Cuando una transacción espera ser verificada, se encuentra en la Main Pool con el resto de transacciones a la espera de verificar. Es de esa Main Pool de donde los mineros van a escoger las transacciones que van a incluir en el bloque que están creando. El minero siempre va a tender a incluir antes las transacciones que incorporan las mayores comisiones antes que las de menor importe dado que ellos van a ser los que reciban dichas comisiones. Puesto que las comisiones son voluntarias, cada usuario elige la comisión que quiere ofrecer a los mineros por su transacción, si el usuario tiene interés en que la transacción se realice lo antes posible (como en el caso de un comercio por ejemplo), entonces ofrecerá de forma voluntaria una comisión superior para llamar el interés de los mineros y que así su

transacción tome lugar lo antes posible. Más adelante veremos la evolución de las comisiones mínimas de Bitcoin que sirven como herramienta para estimular el uso de esta criptomoneda para las transacciones.

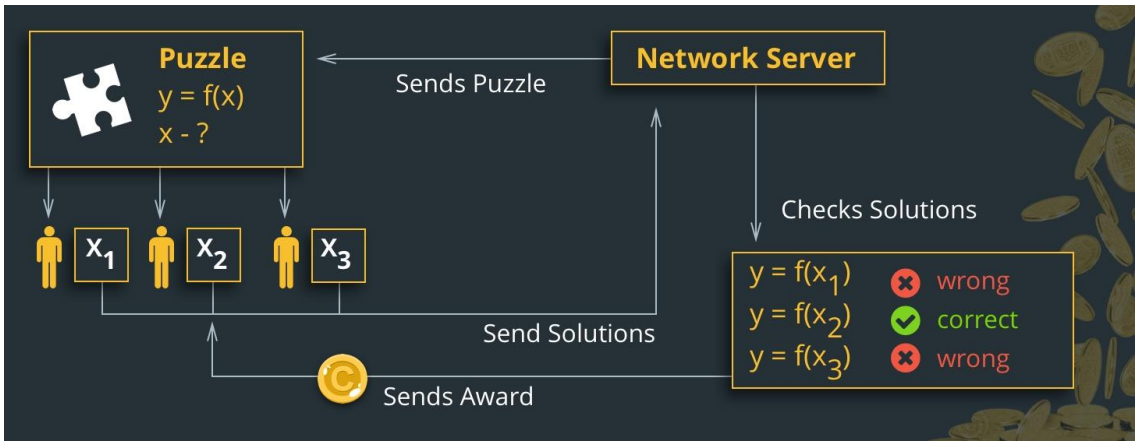
- HashCash para la minería de Bitcoin

Tal y como se mencionó en apartados anteriores, la cadena de bloques Blockchain hace uso del sistema hash para la encriptación e identificación de cada uno de los bloques que componen la cadena. Del mismo modo, en el caso específico de Bitcoin, se hace uso de un sistema HashCash [xviii], por el cual se implementa un Proof of Work mediante el cual se asegura que la creación de un bloque de la cadena, la minería de Bitcoins, es derivada de un gasto de energía y tiempo demostrando así la voluntad del minero de querer crear dicho bloque.
En este caso se utiliza el HashCash implementando la dificultad de los enigmas a resolver para minar Bitcoins, lo que significa un aumento de la cantidad de energía necesaria para conseguirlo, a causa de 24 horas de funcionamiento del hardware[xix].

El sistema HashCash fue creado en 1997 por Adam Back para evitar el recibimiento de emails Spam en el correo electrónico. De esta forma todo mail que mediante unos logaritmos no demuestre que se ha tardado tiempo y dinero en crearse, es decir que no ha sido enviado en masa por un ordenador sin ton ni son, es considerado Spam y enviado directamente a la bandeja de Correo no Deseado evitando así su lectura innecesaria.

En el caso de Bitcoin, el uso de este sistema de algoritmos evita que la red sea falseada, provocando de esta forma que el sistema de minería sea meritocrático y que todo minero reciba la compensación económica que realmente merece. Una vez que el problema a resolver de POW sea resuelto el hash del bloque es creado tras ser verificado por lo que el minero recibe hoy en día 12,5 bitcoins[xx].

Infographic 6: Minería de Bitcoin



Fuente: Página Web de CoinTelegraph [xxi]

En esta imagen podemos ver claramente el proceso, del cual forma una parte fundamental la minería, el sistema Hash Cash y el Proof of Work, que se lleva a cabo desde el momento en el que se solicita realizar una transacción hasta que finalmente esta toma lugar. Tras haber sido verificadas por la red las transacciones que van a formar parte del bloque que se va a crear, Bitcoin crea el problema a resolver por los mineros. Estos intentan resolverlo compitiendo entre ellos para ver quien lo consigue primero.

Una vez crean haberlo resuelto, se envían los resultados a Bitcoin para verificar que estos sean los correctos. El tiempo medio que tarda un nodo (minero) en resolver uno de esos problemas y en crear el bloque es de 10 minutos. El juego se va complicando.
El primero minero en conseguir resolverlo recibe a cambio 12,5 bitcoins.

En los inicios, Bitcoin se podía minar con cualquier ordenador, pero tal y como hemos expuesto antes, con el aumento de creación de Bitcoins acercándose así a su número finito, los "problemas matemáticos" se van dificultando por lo que hoy en día, la minería solo es accesible a individuos con capital suficiente para adquirir ordenadores con procesadores súper potentes.

La dificultad a la cual se somete la creación de Hash, viene dada por el número de ceros que debe de incorporar el hash al principio de su denominación.

Cada Hash se compone de una serie de letras y números que son reunidos al azar e imposibles de estimar de antemano. Cada prueba realizada es bajo un "nonce" siendo

este un numero arbitrario y secuencial que cambia a cada intento (como si fuese el número de intento que se está realizando). Para el mejor entendimiento y explicación de este concepto lo vamos a ilustrar con un ejemplo[xxii].

A la hora de proponer un problema a resolver para la creación de un hash y consecuentemente de un bloque, se decide una serie de condiciones que debe de cumplir ese hash que son aquellas las que deben de buscar un minero antes que los demás.

Esta condición en el caso de Bitcoin es el número de ceros que debe de incorporar un hash al principio. [xxiii]

Con el ejemplo:

Imaginemos que en un bingo hay 100.000 bolas numeradas que pueden salir. Cuando se requiere que un hash contenga una cantidad de ceros determinada, lo que se está implementando es un número ***target****, por lo que cualquier número que sea inferior del target va a resultar válido. En el caso del bingo, si se dice que el target es 009.000 (es decir nueve mil, pero queremos ilustrar que tiene dos ceros delante), entonces todo número que salga que sea inferior a nueve mil va a ser válido por que va a tener como mínimo dos ceros en su numeración. Cuanto menor sea el numero target, es decir, cuantos más ceros tenga este número, más baja será la probabilidad de dar a la primera con la bola adecuada dado que el rango de números validos va disminuyendo. En este caso el nonce sería el número de bolas que llevamos sacadas, la denominación del intento.*

Fuente del ejemplo: Elaboración propia

Este mismo mecanismo (qué en este ejemplo exponemos de forma simplificada) es el usado por HashCash. El problema a resolver por los mineros es encontrar el hash que se pueda considerar válido teniendo en cuenta los ceros requeridos. (Sánchez de Diego) En cada intento de hash encontrado por los mineros, el nonce va cambiando. Únicamente cuando el minero consigue un hash que comience con el número de ceros correcto, entonces este habrá encontrado la "solución al problema", y si lo ha conseguido antes que el resto de participantes, habrá conseguido validar el bloque y por lo tanto recibirá 12,5 bitcoins.

En la esta tabla podemos ver un pequeño fragmento de lo que podría ser un proceso de minería de un bitcoin con un grado de dificultad de 4 ceros (por poner un ejemplo).

Tabla de Ejemplo para ilustrar 1

Nonce	Contenido del Bloque a encontrar	Hash encontrado
1	"Este es el bloque!" 1	8yhbsiu5rjhbc76wn3hVJas
2	"Este es el bloque!" 2	0Hsah54jo9uj34dn82nln23
…	…	…
567	"Este es el bloque!" 567	00005jhhdg4n98ihund9

*Tabla de elaboración propia con datos aleatorios

En este ejemplo podemos ver que un minero debe de ir calculando diferentes hashes hasta dar con el correcto. De ahí que cuanto mayor poder de computo se tenga, más rápidamente se pueden calcular los hashes hasta dar con el idóneo antes que los demás mineros, por lo que mayor es la probabilidad de ser el primero en crear el bloque.

- Initial Coin Offering (ICO):

Al igual que la salida a bolsa de una empresa también llamada IPO (Initial Public Offering), existen las ICO (Initial Coin Offering)[xxiv]. Esto es un instrumento utilizado por las empresas creadoras de criptodivisas como instrumento de financiación con el objetivo de conseguir los fondos necesarios para poder adquirir todo el material necesario y poder a cabo la el lanzamiento de la supuesta criptomoneda (procesadores, mano de obra…)[xxv]. Esta propuesta de inversión viene detalladamente explicada en un "White Paper" escrito por los creadores de la criptodivisa, en el cual se indica cuáles son las características que hacen destacar a esa criptomoneda sobre las más1.500 restantes, al igual que se indica cual va a ser el plan a seguir en cuanto a su desarrollo se refiere (cuando se va a producir el lanzamiento, que sistema de prueba de trabajo va a ser usado para la minería, tiempo estimado para realizar una transacción, etc.). (Mecheba 2016).

Sin embargo, teniendo en cuenta que las ICO de las criptomonedas no cotizan ni se llevan a cabo en un mercado del todo regulado (aunque están comenzando a aparecer derivados que si que cotizan en bolsa como los futuros), este tipo de inversiones llevan

consigo un riesgo muy elevado. Se han dado varios casos ICO que tras haber recaudado importes exorbitantes resultaron ser estafas, resultando en una huida de los supuestos fundadores llevándose consigo los millones robados a los inversores.

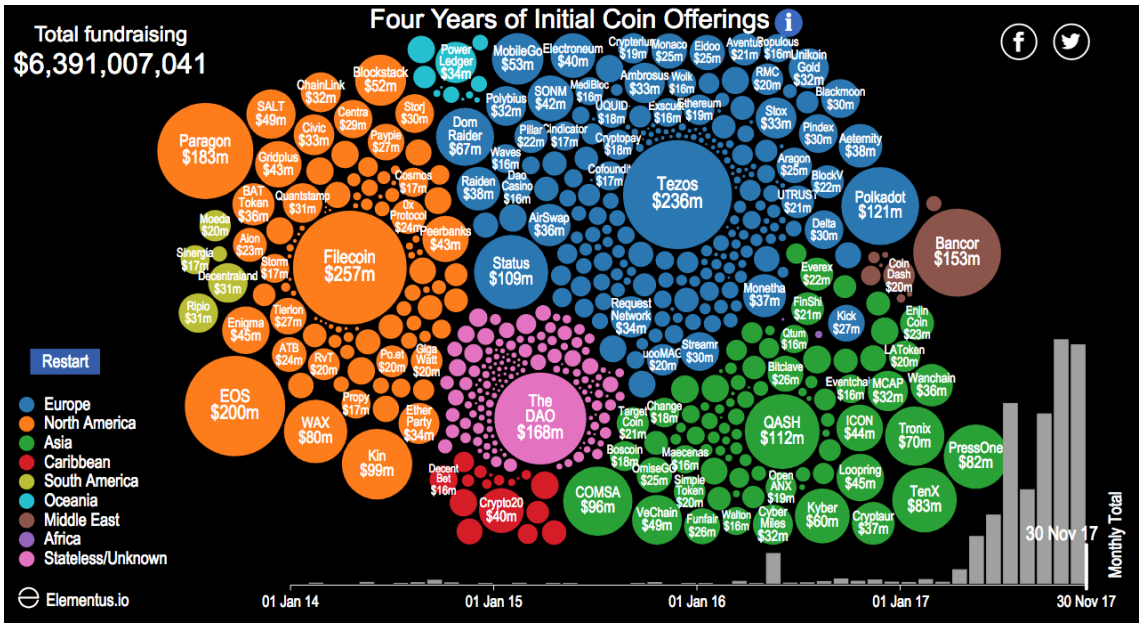
Este es el caso de "Benebit"[xxvi], una ICO que prometía lanzar una criptomoneda que sirviese como instrumento de fidelización de clientes. Tras recaudar entre 2.7 y 4 millones de dólares, se descubrió que las fotos proporcionadas en el WhitePaper del equipo que había desarrollado la criptomoneda eran falsas, por lo que los inversores se vieron estafados sin ninguna posibilidad de recuperar el dinero invertido.

El caso más reciente fue el fallido intento de realizar una ICO de Plexcoin. El pasado diciembre, esta ICO fue suspendida por la SEC (comisión de valores y bolsa de Estados Unidos) alegando que el creador de esta supuesta criptomoneda realizaba una publicidad engañosa asegurando a los posibles inversores un porcentaje de rentabilidad demasiado alto. En el WhitePaper de esta criptomoneda se fundamentaba esta rentabilidad con estudios falsos de analistas y economistas.

La aparición de estas ICO fraudulentas es uno de los motivos por los que, tal y como veremos más adelante, países como China y Corea del Sur han decidido prohibir este tipo de prácticas en sus países.

A pesar de ser una de las herramientas más utilizadas en las estafas de criptomonedas, las ICO siguen siendo la forma más fácil y rápida de conseguir los fondos necesarios para lanzar una nueva criptomoneda. El volumen recaudado por las ICO en los últimos 4 años ha crecido de forma exponencial. Gracias al gráfico interactivo de Elementus.io hemos podido observar que desde 2014 se han recaudado 6.400.000.000 a través de estos instrumento, y de esos millones únicamente 500 millones fueron recaudados entre 2014 y 2016, mientras que los 5.800.000.000$ restantes han sido en el último año. Esto pone en evidencia el creciente interés por parte de la sociedad hacia esta nueva tecnología.

Infographic 7 : Recaudación ICO últimos 4 años



Fuente: Página Web Elementus.io[xxvii]

- Exchange:

Un Exchange es una plataforma de intercambio de criptomonedas a través de la cual se puede acceder siempre y cuando se tenga un monedero virtual donde almacenar las criptomonedas. (Birma 2017) En el caso de Bitcoin, tal y como se explicaba en apartados anteriores, las carteras virtuales permiten almacenar las claves necesarias que indican la posesión de los tokens). (Mecheba 2016) Podemos encontrar una analogía con una casa de cambios donde se pueden intercambiar Bitcoins tanto por otras criptomonedas como por dinero fiduciario (generalmente dólares o euros dependiendo del Exchange usado).

Existen tres tipos de operaciones de intercambio de criptomonedas [xxviii]que indican el tipo de plataforma en la cual se realizan:

- En primer lugar están los intercambios tradicionales de criptomonedas que actúan como una bolsa de valores en la cual se entrega una criptomoneda para recibir a cambio el valor al que se encuentra el cruce en ese momento en divisas como el euro o el dólar. En este caso, el Exchange cobra una comisión por ejercer de intermediario.

- En segundo lugar, las plataformas pueden servir para el intercambio directo entre compradores y vendedores, donde el tipo de cambio que se le da a las criptomonedas no es el fijado por el mercado, sino que es acordado por ambas partes a la hora de realizar la transacción.

- Finalmente están los "Brokers" de criptomonedas. En este caso, el Exchange opera como una casa de cambios de divisas, en la cual los usuarios pueden adquirir o vender criptomonedas, en este caso bitcoins, a un tipo de cambio distinto del de mercado. Este precio va a estar compuesto generalmente por precio de cotización más una pequeña prima que hace de comisión por la función de intermediario ejercida (este es el caso de CoinBase, uno de los exchanges más conocidos).

Para evitar el blanqueo de capitales a través de estas plataformas, en la mayoría de los Exchange es necesaria una identificación de los nuevos usuarios para poder acceder a ésta. Esta medida de seguridad dificulta el uso de las criptomonedas para actividades ilegales como el blanqueo de capitales, permitiendo así que se aumente un poco el control de las transacciones realizadas con este método de pago.

Hay que tener en cuenta que no todos los exchanges permiten un acceso a todas las criptomonedas. Generalmente Bitcoin es la criptomoneda universal por excelencia al haber sido la pionera. Es por esto que la mayoría de los exchanges se puede acceder a esta criptomoneda. Sin embargo en la mayoría de los casos de las más de 1.500 altcoins existentes hoy en día, es muy difícil o costoso acceder a ellas debido a las altas comisiones cobradas por los exchanges que las tienen o a que simplemente hoy en día no se encuentran disponibles en las plataformas que son accesibles públicamente.

¿Qué son exactamente los monederos virtuales?

Al igual que para los Exchange, existen también distintas modalidades de monederos virtuales en los cuales se pueden almacenar las criptodivisas y posteriormente intercambiarlas con motivo de transacción o especulativo. Esto se debe principalmente a las distintas condiciones o voluntades de los usuarios.

Antes de entrar en una clasificación más exhaustiva, podemos clasificar los distintos monederos en dos categorías; los "hot wallets" y los "cold wallets"[xxix]. Podemos considerar los hot wallets aquellos monederos que se encuentran conectados permanente a internet. Está condición "online" convierte a estos monederos en los más prácticos dada su accesibilidad, pero se podrían considerar inseguros puesto que son los más expuestos a ataques y robos. Sin embargo en el caso de los cold wallets ocurre lo contrario, este tipo de monederos están en su mayor parte "off line", es decir que no están conectados a internet, o incluso dada su condición física como es el caso que veremos a continuación de los monederos de papel, en ningún momento llegan a estar conectados a la red. Este tipo de monederos están más protegidos contra ataques pero son menos prácticos.

Dadas estas características, es recomendable el uso de cold wallets en el caso de que se quiera mantener las monedas en el largo plazo mientras que las hot son recomendables en el caso de que se quiera realizar transacciones con estas en el corto.

A continuación estudiaremos más detalladamente las propiedades de cada uno de estos monederos[xxx]:

- **Los monederos de Software o monederos de escritorio:** son monederos que se descargan directamente en el ordenador y dan completa libertad para el manejo de las criptomonedas. Al instalar este tipo de monedero virtual en el ordenador, en el caso de instalar el "Bitcoin Core Protocol", se está pasando a formar parte de la cadena de Blockchain, por lo que todas las transacciones que han sido realizadas desde el lanzamiento de esta deben de ser registradas en el ordenador, lo que conlleva a más de 150gb de memoria.

- **Monederos móviles:** este tipo de monederos son aquellos que nos permiten tener en todo momento las criptomonedas a nuestro alcance puesto que se instalan en los dispositivos móviles. Tanto "Blockchain" como "Bitcoin Wallet" están disponibles para iOS y Android.

- **Online Wallet:** este tipo de monederos no se encuentran en posesión de los usuarios, sino que forman parte de la plataforma de la web elegida para almacenar nuestras criptomonedas. Son bastante prácticos dado que se puede

acceder a nuestro monedero desde cualquier dispositivo conectado a la red y no requiere de ningún tipo de descarga tan solo el conocimiento de usuario y contraseña. Asimismo este tipo de monederos llevan implícito bastante nivel de riesgo puesto que se está usando como almacenamiento de nuestras claves la plataforma de la página web, por lo que en caso de que ésta sea reciba un ciberataque, nuestras claves pueden ser robadas.

- **Monederos en papel:** Este tipo de monederos son los que más se asemejan a un monedero convencional dado que se encuentran en un estado físico. En términos generales, este tipo de monederos son documentos impresos en papel en los cuales está escrita toda la información que demuestra la posesión de una criptomonedas (claves públicas, privadas, firmas digitales, etc.). Este tipo de monederos son muy dado que no pueden ser robados en un ciberataque, sin embargo cabe la posibilidad de pérdida al tratarse de un activo físico.

- **Monederos Hardware**[xxxi]: estos monederos también son monederos físicos. Sin embargo, estos no son documentos impresos, sino que son como pequeños discos duros que constan con un chip criptográfico al que únicamente se puede acceder con unas claves privadas. Este tipo de wallet nos da la oportunidad de tener un control total sobre nuestras criptomonedas, teniendo una conexión puntual con internet (únicamente cuando se desea realizar un intercambio) por lo que también están protegidos de los ciberataques.

Los desarrolladores de Bitcoin

La Blockchain de Bitcoin hoy en día es la más potente y más segura de todas las que se encuentran en el mercado. Tal y como nos indicaba Iñigo Molero en la entrevista:

> *"El éxito de una Blockchain se sustenta en tres patas:*
> *- La seguridad: los mineros. Bitcoin hoy por hoy es la Blockchain pública más segura del mundo. La capacidad de cómputo que tiene es abismal y si alguien quiere hackearlo*

> *tiene que meter una capacidad de cómputo que es imposible.*
>
> *- La comunidad: la gente que soporta una criptomoneda. Bitcoin tiene una comunidad más beligerante, la primera de todas y la que más que cree en esto que estamos haciendo*
>
> *- Los desarrolladores: gente de inmenso talento que está continuamente trabajando para mejorar el código. Por ejemplo: RSK, una empresa argentina que en diciembre sacó un prototipo para sobre la Blockchain de bitcoin para hacer contratos inteligentes (como lo que hace Ethereum).”*
>
> (Molero 2018)

Estos últimos, los desarrolladores son los que sostienen el sistema.

La vitalidad del ecosistema de Bitcoin consiste en un torrente de imaginación que hay para la resolución de los problemas que resulta en una mejora continua del sistema. Los desarrolladores de Bitcoin consiguieron varias soluciones para la falta de escalabilidad (capacidad de reacción y adaptación sin pérdida de calidad antes grandes volúmenes de transacciones a la vez). Entre estas soluciones se encontraban las siguientes:

- En vez de que los bloques fueran de un mega, hacerlos 8 megas. Sin embargo esto sacaba de la ecuación a los nodos con poca capacidad de cómputo donde descargarse una cadena tan pesada. La fortaleza de la red te la da que haya muchos nodos participen, que este muy descentralizado.
- Segwit y Ligthning Networks (una sidechain). Los que apostaban por sidechains.
  Segwit te ofrecía quitar ciertos datos del hash, hashearlos restructurarlos, quitando parámetros que no eran del todo importantes, y ganar un 75% más de capacidad sin mover los parámetros de un bloque. Todo ello sobre la cadena de bitcoins, en vez de hacer el bloque más grande, optimizarlo.
  Ligthning Networks es una sidechain. Esto significa que permite abrir cadenas laterales. Abres un canal de pago en Ligthning, se congela el saldo de Bitcoins en la cadena principal. Es como una especie de canal de pagos por fuera de la cadena. Cuando se cierra el canal, se introduce el nuevo saldo en la cadena madre habiendo ahorrado saturar la cadena de bloques principal de pequeñas transacciones. Esta

sidechain es igual que la Blockchain original, mismas condiciones de seguridad y de trazabilidad (Molero 2018).

Gracias a los desarrolladores, la Blockchain de Bitcoin se ha ido desarrollando de forma que ha ido incorporando a su cadena sidechains que han permitido obtener características que otras criptomonedas ya ofrecían. Este es el caso por ejemplo de RSK que permite hacer contratos inteligentes en la cadena como Ethereum o MimbleWimble (en proceso de simulación) que permite realizar transacciones con Bitcoin de forma **completamente anónima,** tal y como realizan ya otras criptomonedas del mercado como Zcash o Monero.

Tras haber estudiado en profundidad cuales son las características de ésta revolución tecnológica que son Blockchain y Bitcoin, cabe preguntarse qué futuro tiene este nuevo internet del valor en la economía actual que desmaterializa el sistema financiero. Para poder estudiar esto, vamos a dividir el segundo bloque en tres bloques diferentes que nos van a permitir analizar, la condición de dinero que puede tener esta criptomoneda, la posible regulación de Bitcoin y finalmente si se puede considerar que nos encontramos ante una burbuja especulativa.

CONSIDERACIONES SOBRE BITCOIN

¿SE PUEDE CONSIDERAR A BITCOIN DINERO?

En el siguiente apartado, gracias a las funciones básicas que debe de cumplir toda moneda en su sentido más estricto para que sea considerada dinero, podremos analizar el nivel de aceptación que tiene Bitcoin a la hora de considerarlo dinero. Estas funciones básicas son unidad de cuenta, medio de pago y reserva de valor. (Yermack 2014)

Unidad de cuenta y patrón de precios:

A la hora de realizar una transacción, el uso del dinero facilita la realización de ésta, disminuyendo los costos relacionados en vista que reduce los diferentes precios existentes en la economía. Para que Bitcoin cumpla la función de unidad de cuenta, esta criptomoneda debe de servir como unidad de medida en la que se expresan los precios

de todos los bienes y servicios del mercado a la hora de querer compararlos con otros bienes sustitutivos. (Mecheba 2016)

Dada la alta volatilidad que sufre diariamente Bitcoin, esta condición es dudoso que se cumpla. Los comerciantes deben de recalcular constantemente el valor de los bitcoins que tienen en su poder o que van a adquirir para tener su cartera actualizada y saber el poder adquisitivo que tienen con esta.

Sin embargo, aunque el uso que se le puede dar a Bitcoin como unidad de cuenta dificulta bastante las transacciones por su permanente cambio, puesto que ésta criptomoneda tiene un tipo de cambio cotizado en dólares y más divisas, teóricamente si que podría considerarse que se cumple esta función.

Medio de pago:

Esta función expresa el hecho de usar el dinero como medio para el intercambio de valor para una transacción. Para ello, debe de cumplir dos cualidades. En primer lugar que sea **homogéneo (fungible)** (Birma 2017). Esta condición Bitcoin la cumple dado que aunque las claves de cada bitcoin o su almacenamiento difieran, finalmente todas las unidades siguen un protocolo y tienen el mismo valor en su totalidad (el título de propiedad del token no influye en su valor).

Asimismo, una moneda debe ser **divisible y transportable**.
Los bitcoins son **divisibles**: no tiene que permanecer necesariamente como una unidad única y completa, sino que se puede dividir en porciones que están a la venta y sirven para las transacciones del mismo modo que un Bitcoin. Estas pequeñas porciones son las mencionadas en apartados anteriores los Satoshis, en honor a su creador.
Finalmente, un bitcoin es completamente **transportable**. Esto ya viene implícito con la red de cadenas de bloques (Blockchain) utilizada por Bitcoin. Por lo tanto esta criptomoneda es completamente transportable tanto en su plenitud (un Bitcoin) como en su aspecto fraccionado (un Satoshi).

Reserva de Valor:

Se podría afirmar que la función de reserva de valor es la más relevante dado que de ella que resulta el nivel de confianza que los usuarios depositan en esta moneda.
Para que se cumpla está función, al igual que las otras, se deben cumplir ciertas propiedades.

- En primer lugar la reserva de valor debe de ser **duradera.** La moneda debe de poder ser utilizada como un medio para mantener el valor del patrimonio a largo plazo como pueden ser los ahorros de una persona. De ahí la denominación de reserva de valor. En el caso de Bitcoin, dada su alta volatilidad sobretodo en el último trimestre donde la valoración de Bitcoin ha caído en más de un 60%, podríamos afirmar que la reserva de valor que ejerce Bitcoin no es duradera (los niveles de especulación se verán más adelante en este informe) (Mecheba 2016).
- Del mismo modo, debe de ser **difícil de falsificar**. Gracias a los métodos criptográficos con los cuales se crea y se realizan transacciones con ella, podemos afirmar que Bitcoin sí que cumple esta propiedad.
- Finalmente, debe ser un **bien escaso**. Esta característica viene cumplida originalmente por el número finito de tokens que pueden ser creados impuesto por su creador Satoshi Nakamoto.

El propósito de este análisis no es el de demostrar que los bitcoins no deben de ser utilizados como dinero, sino que se quiere exponer que estas criptomonedas no cumplen con todas las funciones necesarias para adquirir ésta condición.

Cabe destacar en el caso del dinero fiduciario, a pesar de que en la teoría sí que es mundialmente considerado dinero por su procedencia y respaldo por parte de los bancos centrales, en la práctica podría decirse que estas divisas también incumplen algunas de estas funciones, aunque en menor medida, dado no cumplen totalmente esta función de reserva de valor.

Por una parte, el **dinero fiat** a causa de las políticas monetarias realizadas por los bancos centrales, las monedas sufren cambios en la valorización de la moneda, es lo que se denomina inflación (en el largo plazo), afectando así a la reserva de valor realizada con el uso de estas monedas. El valor del dinero cambia constantemente, por lo que

cambia el poder adquisitivo de las personas (mil euros hoy en día pueden permitirme comprarme más cosas que dentro de un año). En el caso de Bitcoin dada alta volatilidad que mencionábamos anteriormente, se tienen en cuenta franjas de tiempo mucho menores (incluso intra-día). No se puede asegurar que el valor del importe de una venta con pago realizado en Bitcoins va a ser el mismo hoy que mañana. La única forma de garantizar que se reciba el importe por el que se ha vendido el bien sería intercambiar los Bitcoins por dinero fiduciario en el mismo momento de recibimiento de los tokens.

En la entrevista con Iñigo Molero, él mismo nos decía:

> *"Si tú te fijas en las características del dinero: divisible, escaso y fácil de transportar, Bitcoin ha sido capaz de optimizar todas estas cosas."* (Molero 2018)

Tabla de Ejemplo para ilustrar 2

	ORO	*FIAT*	*BTC*
Divisible	*no*	*si*	*si*
Escaso	*si*	*no*	*si*
Fácil de transportar	*no*	*si*	*si*

Motivos de demanda de Bitcoin.

Para finalizar este análisis sobre la utilidad que se le da a Bitcoin como dinero, cabe estudiar cuales son los motivos por los que se poseen o se quieren poseer estas criptomonedas.

Dado que se trata de un sistema completamente descentralizado, Bitcoin no ofrece mucha información sobre la identidad e intenciones de sus usuarios. Sin embargo, gracias al estudio que hemos ido realizando a medida que avanzábamos en este informe, podemos agrupar los usuarios de bitcoin en tres subcategorías:.

- En primer lugar la minería. Los mineros representan un gran porcentaje de los propietarios de Bitcoin. Estos informáticos han conseguido crear los bloques de la cadena en los que se han incorporado las nuevas transacciones y a cambio han recibido bitcoins (recordamos que la recompensa hoy por hoy es de 12,5 BTC y que

cada año esta cifra se reduce a la mitad). Una porción de los propietarios que existen actualmente de Bitcoins son **los mineros**. Estos usuarios, también denominados early adopters, son aquellos que minaron los primeros bitcoins de forma prácticamente gratuita. Algunos ejercen de holders sin vender para ver que pasa, mientras que otros deciden vender dados las posibles plusvalías. A este subgrupo los podemos denominar "frikis" de los bitcoins que no quieren deshacerse de ellos dado que es su creación, fruto de su trabajo.

- Por otra parte, existen los **usuarios con motivo de transacción** (Mecheba 2016) que adquieren bitcoins con el objetivo de hacer uso de ellos como método de pago. En este caso cabe hacer mención de que esta función de medio de pago que cumple bitcoin únicamente se da siempre y cuando ambas partes involucradas acepten de la misma forma a bitcoin como una moneda. Con el uso de esta criptodivisa los usuarios se ahorran los costes de transacción que van ligados a la intervención de terceros (comisiones de los bancos). Del mismo modo la rapidez con la que se realiza la transacción, tanto si es nacional como internacional, beneficia al usuario agilizando todo el proceso de venta o compra de un activo.

- Finalmente, existen los usuarios que poseen esta criptomoneda por **motivos de especulación**. Tal y como veremos en el próximo apartado, los tipos cercanos a cero tienen como resultado una sobresaturación de liquidez en el mercado con pocas oportunidades de inversión por lo que las criptomonedas dada su alta volatilidad son muy atractivas. Es por esto que una gran parte de los usuarios que hoy en día poseen Bitcoin tienen como único objetivo especular dados los márgenes de beneficios que ha llegado a alcanzar con este activo.

Es por este último motivo de especulación y por los datos exorbitantes de revalorización de esta criptomoneda en el último año, que se plantea la cuestión de que nos encontremos frente a una burbuja especulativa no muy diferente a las vividas en el último siglo como las puntocom o las hipotecas subprime.

¿ES POSIBLE UNA REGULACIÓN DE BITCOIN?

A pesar de que hoy por hoy no existe una regulación común vigente, se ha visto conveniente poner en evidencia en el informe las posturas de las grandes entidades financieras internacionales sobre esta nueva red de pago que tergiversa la forma de intercambio de información y de valores entre los agentes económicos.

¿Por qué se quiere regular Bitcoin?

Al plantearle esta pregunta a Iñigo Molero, este nos dijo:

> *"Se podría decir que los bancos han llevado a cabo las fases de negación que se la tribuyen a Gandhi:*
> - *Primero te ignoran: se hace caso omiso de esta tecnología diciendo que esto es de frikis.*
> - *Segundo: Se ríen de ti*
> - *Te combaten: Alegando "esto es de terroristas, burbuja especulativa, etc."*
> - *Te ganan o se unen: intentan meter Blockchain en sus sistemas para optimizar sus propios procedimientos (teniendo que llevarse a cabo esto primero con una regulación)* (Molero 2018)

Tal y como se ha expuesto anteriormente, dado el volumen de mercado y la importancia que se le ha dado en los últimos meses al uso de criptomonedas como medio de pago, cada vez se hace más fuerte una presión generalizada por parte de los Estados de una regulación común para este tipo de divisas digitales al igual que aumenta las posibles repercusiones que pueden tener estas criptomonedas en la economía.

Bitcoin es el foco de todas las miradas dado que es la pionera de las criptomonedas dado que se trata de la criptomoneda principal por excelencia necesaria para un primer acceso a la mayor parte de las demás altcoins y la que más volumen de mercado tiene.

Del mismo modo Bitcoin aparece en un momento donde los agentes económicos buscaban alternativas al sistema financiero que les había engañado y metido en una crisis económica mundial por las hipotecas subprime.

La principal razón por la que se está exigiendo que este tipo de moneda digital sea regulada de alguna forma, es justamente la condición distribuida y descentralizada que la diferencia del resto de divisas legales ya existentes (euro, dólar, etc.) que están respaldadas por las economías. Tal y como se ha expuesto anteriormente en este informe, bitcoin hace uso de la cadena de bloques Blockchain para el registro y la puesta en acción de sus transacciones. Al tratarse de una cadena distribuida y descentralizada, no está ligada a ningún Estado ni economía, por lo que permite a los usuarios realizar movimientos de capital sin ningún tipo de regulación ni control, incluyendo anonimato a las transacciones. Es a causa de esto que se teme que las criptomonedas sean usadas para el blanqueo de capitales, la evasión de impuestos o la financiación de actividades ilegales como el narcotráfico o terrorismo.

Un ejemplo de esto fueron los anuncios publicados el pasado diciembre por el Estado Islámico (ISIS) en los cuales se animaba a los simpatizantes de este grupo terrorista a donar de forma anónima cualquier cantidad de bitcoins para financiar sus actos. Para ello en el póster se indicaba la clave pública del monedero de Bitcoin al que debían ser enviadas las criptomonedas junto con una frase motivadora procedente del Corán[xxxii].

Del mismo modo, al tratarse las criptomonedas de un activo confuso y con una tecnología de difícil comprensión, los Estados temen por sus ciudadanos al exponerse a este tipo de riesgos. Así mismo, el contribuyente no es el único en verse expuesto a un riesgo al invertir en algo tan volátil[xxxiii] como la criptomoneda, sino que las instituciones gubernamentales se ven afectadas puesto que existe una evasión de impuestos que afecta directamente a la recaudación recibida por los Estados. Un ejemplo claro de esto ocurrió en 2015 donde únicamente 807 personas declararon los impuestos procedentes de Bitcoin [xxxiv].

Hoy en día no existe ninguna regulación vigente internacional que permita limitar y controlar todo el mercado que lleva consigo el mundo de las criptomonedas. Sin

embargo, a pesar que la falta de regulación común, ciertos países están llevando a cabo medidas para que este tipo de activos desaparezcan en el interior de sus fronteras.
Iñigo Molero nos explicaba las distintas posturas que están teniendo los países ante esta nueva tecnología.

> *"Hay varias posturas:*
> *- Los países que acabamos de mencionar que dicen: Esto va ser una revolución extraordinaria, las próximas grandes multinacionales van a estar sobre Blockchain. Vamos traer esta tecnología a nuestro país y así creamos riqueza y puestos de trabajo.*
> *- Países que no saben muy bien que hacer como España que hará lo que decida la Unión Europea.*
> *- Países como China que prohíben estas prácticas porque se les va de las manos. Los prohíben como forma de regularlo"* (Molero 2018)

¿Cómo se puede regular Bitcoin?

Una de las primeras medidas de control sobre criptomonedas vino de la mano de China, el cual prohibió el pasado septiembre la participación de sus ciudadanos en la recaudación de fondos de una ICO. Con esto se intenta frenar el lanzamiento de nuevas criptomonedas que refuerzan este mercado de capitales virtual que es ajeno al control del Estado chino. Más adelante en Corea del Sur tomó la misma medida con el pretexto de que se debía controlar de alguna forma este mercado al observar que las recaudaciones de este instrumento de financiación llegaron a los 4 mil millones de dólares. Este tipo de controles se llevan a cabo impidiendo el acceso de los ciudadanos a las plataformas internacionales de criptomonedas e imponiendo sanciones a todos aquellos que participen en una ICO.

Sin embargo, estas medidas no están teniendo el resultado esperado puesto que los inversores al verse privados de las plataformas convencionales, hacen uso de otros instrumentos tales como los grupos de discusión QQ, Telegram o Wechat [xxxv] en los cuales se llegan a acuerdos de intercambio de criptomonedas.

Estos proyectos de regulación o medidas impuestas, afectan gravemente a la cotización de las criptomonedas. Ante la regulación impuesta en de Corea del Sur, siendo éste el país que realiza un quinto de las operaciones de criptomoneda, provocó una venta masiva de Bitcoins, Ethereum y demás altcoins, resultando en una caída en su cotización en más de 20%.

La medida más actual que podemos encontrar es la última declaración de Google en la que se indica que a partir de junio, el motor de búsqueda más potente del mundo prohibirá cualquier tipo de publicidad de criptomonedas o ICO en los países cuya legislación prohíba este tipo de inversión[xxxvi].

La condición de anonimato de esta red, dificulta la regulación dado que la identidad de los usuarios que participan en las transacciones no es revelada. Sin embargo existen organismos como ChainAnalysis que se dedican exclusivamente a identificar posibles fraudes fiscales gracias a la trazabilidad de las transacciones.

En el marco teórico, una legislación común podría llegar a ser posible. Sin embargo, a pesar del descontento existente en la mayor parte de los países por el uso de las criptomonedas y las actividades ilegales que incitan, existen también otros países que mantienen una postura completamente opuesta dado que quieren adoptar la tecnología Blockchain[xxxvii]. En este segundo a favor de estas divisas digitales, los Estados quieren crear las suyas propias o invertir en algunas ya existentes.

Si no puedes vencerles, únete a ellos

Aunque las criptomonedas sean vistas como un activo demasiado volátil que tal y como veremos más adelante en este informe se pueden considerar una burbuja especulativa, ciertos Estados se han visto atraídos y están invirtiendo en la tecnología de Blockchain alegando que éste internet del valor representa al futuro. Es por esto que algunos países estudian la adopción de la cadena bloques junto con la creación de criptodivisas respaldadas por los bancos centrales para sus sistemas financieros.

El lanzamiento de una criptomoneda que esté respaldada por el banco central de un país, sería ir en contra de la condición distribuida y descentralizada de las

criptomonedas. Sin embargo la aplicación de este sistema de pagos virtual beneficiaría a los sistemas financieros teniendo en cuenta la rapidez de verificación de las transacciones y la disminución de los costes transaccionales permitiendo así que cualquier operación pueda tener lugar sin estar limitado por los horarios de los distintos países. A la hora de implementar una criptomoneda de un país existirían dos modalidades:

- En primer lugar la criptomoneda mayorista[xxxviii] sería aquella utilizada a la hora de querer realizar grandes operaciones entre bancos o con el banco central. El uso de esta red de pagos permitiría un registro de todas las transacciones que sería directamente enviado al banco central por lo que se evitaría el control realizado al solapamiento de transacciones interbancarias. Sin embargo, el uso de criptomonedas disminuiría el nivel de negocio realizado por la banca convencional por lo que esta se esta última se vería gravemente perjudicada.

- Seguidamente la criptomoneda minorista sería de uso público por lo que podría resultar en la eliminación de efectivo en los Estados.

El uso de criptomonedas nacionales tiene una serie de beneficios a la hora de querer implementar las políticas monetarias de un país. En el caso de que se quieran aumentar o disminuir los intereses, la digitalización de las divisas hace más efectiva la implementación de nuevos tipos afectando directamente a toda la masa monetaria.

Hoy en día el uso de las criptomonedas respaldadas por los bancos centrales no es más que un proyecto que solo existe en la teoría, aunque países como Suecia están realizando estudios para su implantación inmediata.

Sin embargo, las criptodivisas nacionales no son la única forma de adoptar la cadena de Blockchain en los sistemas financieros. Existen algunos casos en los que las grandes instituciones financieras ya han apostado por las criptomonedas habiéndolas incluido en sus sistemas o invirtiendo en ellas.

- Ripple, la criptomoneda de los bancos

  Ripple[xxxix] es uno de los ejemplos más característicos de esta inclusión de las criptomonedas en los grandes bancos. Esta criptodivisa ofrece la posibilidad de realizar transacciones financieras de forma global permitiendo así liquidar, recibir y enviar transacciones de forma rápida (unos 10 segundos) al igual que permite cambios a otra divisa o criptomoneda. Se dice que Ripple es la criptomoneda de los bancos puesto que ha conseguido acuerdos con algunos de los bancos más influyentes y con más peso en el mercado tales como Santander, BBVA y Bank of America. Una de las razones por las que esta altcoin es atractiva por los bancos es que a diferencia de otras criptomonedas como Bitcoin, esta no es minada por sus usuarios sino que es minada por Ripple Labs por lo que se asemeja al dinero fiduciario en este sentido. Esta condición garantiza que el uso y creación de esta criptomoneda no es puramente especulativo, dado que la oferta que hay en el mercado está completamente controlada por su sistema central Ripple Labs.

Como podemos observar la regulación de las criptomonedas se encuentra todavía en fase experimental existiendo varias posturas a la hora de llegar a un acuerdo para regular esta nueva tecnología que puede representar el futuro de las transacciones financieras. Por un lado están los Estados que presionan cada vez más para una regulación inminente dadas las repercusiones que pueden tener estas monedas digitales por su anonimato y su volumen de mercado, mientras que otros Estados y en especial grandes bancos se han visto atraídos por Blockchain y su sistema de pagos inmediatos, P2P y con un coste transaccional bajo. A su vez, gran parte del mercado de criptomonedas desea ser regulado dado que esto supondría una inyección de capital institucional.

Más adelante, estudiaremos en profundidad el efecto que puede tener la regulación en la valorización de los bitcoins pudiendo ser este el motivo por el cual en los últimos dos meses la cotización ha bajado en picado.

Pero, además de considerarse un activo muy volátil y que da rienda suelta a la realización y la financiación de actividades ilegales, ¿podría decirse que Bitcoin y las demás criptomonedas son dinero?

¿ES BITCOIN UNA BURBUJA ESPECULATIVA?

La alta volatilidad de los últimos años, ha ido generando el debate de si Bitcoin es una burbuja especulativa, o si de verdad todas sus valoraciones están fundamentadas y este activo va a tener perpetuidad dados sus posibles usos. Es por ello que en este informe hemos visto conveniente analizar si esta criptomoneda cumple las características de una burbuja haciendo un estudio según el modelo de Crisis Financiera de Minsky[xl] en el cual se hace una distinción de las diferentes etapas por las que transcurren las burbujas especulativas, y los motivos por los cuales Bitcoin ha sufrido una fuerte especulación en el último año.

Al tratarse Bitcoin de un tipo de moneda completamente nueva de la cual no se tiene antecedentes, no se puede analizar el efecto que ha podido tener otros activos similares en la economía por lo que en este apartado se va a trabajar con los datos históricos disponibles desde la aparición de esta criptomoneda.

En el momento de su lanzamiento, Bitcoin causó mucha polémica dada su innovadora y compleja tecnología que resultaba en una falta de comprensión por parte de los inversores que no entendían muy bien el funcionamiento de esta nueva red de pago descentralizada y anónima.

La razón por la que se ha buscado el entendimiento de todos los elementos de esta criptomoneda a lo largo de este informe es justamente poder argumentar con fundamento un estudio más profundo de las razones por las cuales bitcoin podría considerarse una burbuja especulativa que podría explotar, si no es que ha explotado ya.

Mismos antecedentes

Si algo nos enseña la historia económica, es que las burbujas financieras siempre se inician en situaciones económicas similares. Los agentes económicos son propensos a invertir en activos de alto riesgo en momentos donde la financiación es muy barata y

existen pocas posibilidades de inversión. En estos casos la economía es estable, por lo que no es frecuente encontrarse con activos con rendimientos más altos de lo normal por lo que en cuanto surge alguna innovación, ésta llama la atención de los inversores que deciden apostar por ella. Se produce una migración hacia estructuras de financiación más agresivas.

Analizándolo cronológicamente, tras la explosión de la burbuja especulativa de las puntocom, hubo un aumento de paro y se bajaron los tipos a mínimos históricos para facilitar la financiación de los bancos. Esta facilidad de financiación resultó en un exceso de liquidez que tan solo unos años después provocaría la segunda burbuja especulativa a tratar, la crisis de las hipotecas subprime. Esta burbuja no sólo tergiverso la economía de los países afectados por estas hipotecas basura, sino que tuvo repercusiones en la economía internacional, derivando en una serie de políticas monetarias en los principales bancos centrales como la Reserva Federal y el Banco Central Europeo, tal y como podemos observar en los dos gráficos expuestos a continuación. Estas políticas monetarias consistían en una bajada de tipos en 2008 alcanzando el 0,250%[xli] (siendo este su mínimo histórico) para la Fed y el 2,5%[xlii] en el caso del Banco Central europeo se siguió disminuyendo hasta alcanzar los tipos cero.

Gráfico 1: Tipos de la Reserva Federal (Fed) desde la Crisis Económica de 2008

Fuente: Página Web Macrotrends[xliii]

Gráfico 2: Tipos del Banco Central Europeo (BCE) desde la Crisis Económica de 2008

Fuente: Página Web TradingEconomics[xliv]

Esta crisis es una de las más destacables dentro de las crisis económicas y financieras dado que fue una crisis económica mundial que afectó de manera internacional a todas las economías.

Sin embargo, esta bajada de tipos no afecta únicamente al coste de financiación tanto de los bancos como de los agentes, sino que también disminuye las tasas de rendimientos de los mercados. Es por esto por lo que los inversores se ven atraídos por activos que, aunque supongan un mayor riesgo les ofrezcan un margen de beneficios superior actuando en base a la especulación, como puede ser el caso de Bitcoin. (Entrecanales 2014)

La crisis subprime no solo afectó a la economía en términos cuantitativos, sino que también provocó una sensación de desconfianza hacia las instituciones financieras dado que habían sido estas las que habían llevado la economía mundial prácticamente a la ruina tras una época de expansión provocada por una burbuja especulativa respaldada por un engaño generalizado de las hipotecas subprime.

Fue en 2009, tras la explosión de la burbuja especulativa de las hipotecas subprime que aparecen Blockchain y Bitcoin, una nueva forma de realizar transacciones de forma segura y descentralizada junto con un modelo de criptodivisa jamás visto hasta la fecha

dada su condición de anonimato. Estas innovaciones responden a esa demanda de actuación ajena al sistema financiero convencional. (Mecheba 2016)

Sin embargo, al no tener un Banco Central o economía que lo respalde, Bitcoin es altamente volátil. Dada su falta de condición física, Bitcoin no es más que una serie de números por lo que su precio está marcado por el cruce entre la oferta y la demanda de esta criptomoneda. Es a causa del numero finito de oferta impuesto por su creador Satoshi Nakamoto, por lo que se podría considerar los bitcoins como un bien escaso, derivando esto en que cualquier cambio en la demanda de bitcoins va a tener un efecto inmediato en la valoración de la criptodivisa.

Adicionalmente, otro de los factores que tienen un gran peso en la cotización de bitcoin es la expectación de revalorización futura de este activo. (Mecheba 2016) Tanto si el objetivo es usarlo como medio de pago como si es el de vender el bitcoin en un momento de cotización superior al de compra (especulación), los usuarios solo van a adquirir esta criptomoneda bajo la suposición de que la valoración de esta va a subir[xlv]. Esta determinación del precio basada en las expectaciones de cotización de un activo, es una de las características fundamentales para la creación de burbujas especulativas. Es por ello por lo que a continuación procederemos a un análisis según el modelo de Crisis Financiera de Minsky, en el cual observaremos las distintas fases de una burbuja especulativa buscando una analogía entre este tipo de crisis y la valoración de bitcoin.

Analogía de valoración de Bitcoin con Crisis Financiera de Minsky

Antes de entrar en el estudio de este modelo de crisis financieras, queremos destacar que éste siempre se va a realizar partiendo de la base de que tal y como exponía George Soros en 2010, en "la economía no existe una verdad objetiva por lo que no existe una solución correcta e inevitable" (Entrecanales 2014). Es por esto por lo que sea cual sea el resultado del estudio que se va a exponer a continuación, éste no va otorgar una respuesta rotunda a la pregunta formulada, sino que va a exponer hechos fundamentados que facilitarán el posterior juicio del lector una vez se le haya expuesto todos los datos.

Minksy escribía que toda crisis financiera seguía una serie de patrones cíclicos que permitían identificarlas incluso antes de su implosión[xlvi].

- **Planteamiento:** (Noguera 2006) Esta fase pone en evidencia el descubrimiento de un nuevo producto o innovación tecnológica que en este caso sería Blockchain y Bitcoin. Para que éste descubrimiento tenga relevancia, se tiene que creer que este nuevo producto pueda tergiversar la economía tal y como la concebimos hoy en día. Refiriéndonos a Bitcoin, un sistema de pagos descentralizado, anónimo y ajeno al sistema financiero hizo pensar que cambiaría el modo de realizar transacciones convencionales del sistema financiero que hasta entonces se conocía en 2009 tras su lanzamiento.

- **Comienza la subida de precios:** aunque esta subida es casi imperceptible para Bitcoin, se empieza a correr la voz de esta nueva divisa digital que llama la atención de los inversores. Al comienzo al existir una oferta muy limitada puesto que había pocos tokens "creados", un aumento de la demanda hizo que aumentase su cotización, aunque esta no llego a alcanzar una unidad de dólar completa en todo 2010 ($1.00)

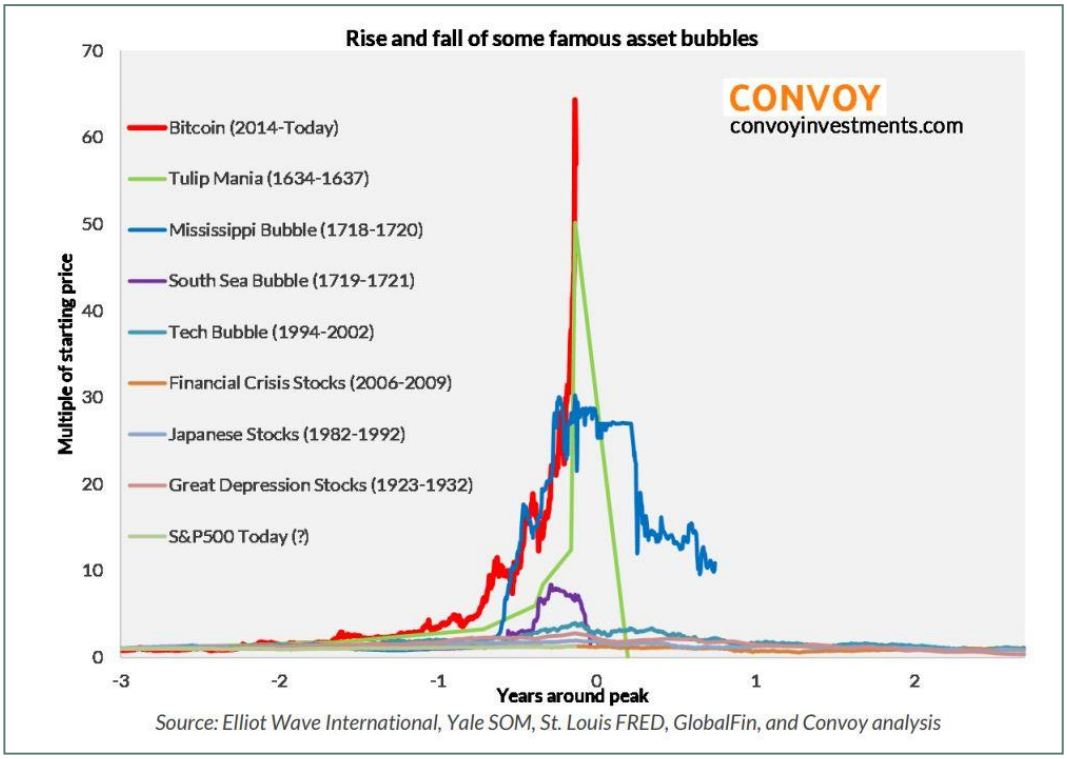
- **Crédito fácil:** tal y como se ha indicado en apartados anteriores, ante una situación de crisis económica mundial los principales bancos centrales bajaron los tipos a sus mínimos históricos (volver a observar el Gráfico 1 y Gráfico 2) en 2009 justo en el momento de aparición de Bitcoin, aunque esta bajada no comenzó a tener repercusiones hasta años posteriores. La posibilidad de crédito fácil provoca la invasión de los agentes externos en este nuevo mercado "creando así la burbuja financiera".(Sanchis 2008)

- **Recalentamiento del mercado:** Como resultado de esta bajada de tipos, los volúmenes de operaciones son estimulados mientras que la oferta de bitcoins sigue estando bastante acotada por el corto periodo de vida de esta criptomoneda. Esto provoca que la especulación comience a ser fructífera haciendo más atractivas las inversiones en la criptomoneda de forma que Bitcoin empieza a crearse un hueco en el mundo de la inversión.

- **Euforia:** Es en esta etapa donde la burbuja está en pleno apogeo. Los precios se han disparado llegando en 2017 a casi 20.000$ el precio de cotización de un bitcoin e incluso llegando a una revalorización de casi tres mil dólares de un día para otro. La

mayor parte de los agentes económicos quieren invertir en esta criptomoneda que sin explicación racional a alguna se ha visto con una revalorización sin precedentes en la economía actual. Sin embargo, lo que no quieren ver los agentes es que este tipo de revalorizaciones únicamente han sido vistas en momento de auge de los activos que provocaron las mayores burbujas especulativas de la historia. En el siguiente gráfico, podemos apreciar que la revalorización de Bitcoin y la especulación ha llegado a superar a las grandes burbujas anteriormente mencionadas. En el gráfico aquí expuesto el "año 0" corresponde a la etapa de euforia a finales de 2017 en los cuales Bitcoin alcanzó su cotización máxima de $19.205 según exchanges como CoinBase[xlvii]. (Cabe destacar que cada Exchange expone cotizaciones diferentes de las criptomonedas dadas las comisiones cobradas, tal y como se explicó en apartados anteriores).

Gráfico 3: Analogía de Bitcoin con burbujas especulativas de la histori



Fuente: "Why Bitcoin is now the biggest Bubble in history in one chart" Web MarketWatch[xlviii]

Teniendo en cuenta esta comparativa con crisis financieras de especulación anteriores no es de extrañar que existan ciertas opiniones de que no cabe duda que nos encontramos ante una burbuja especulativa.

- **<u>Los expertos recogen beneficios</u>:** Aquí es donde entra la expresión que caracteriza este modelo de crisis financiera de Minksy "tonto el último"[xlix]. Los inversores que poseen estas criptomonedas las venden ante una revalorización de tal calibre. Los márgenes de beneficios son impresionantes. Un individuo que hubiese adquirido el 1 de enero de 2017 un bitcoin por $961,30 el 16 de diciembre (ni siquiera un año después) lo vendió por $19.711,40 (Cotización extraída de CoinMarketCap[l]) obteniendo unas ganancias de $18.750,1, es decir una revalorización de más de 1.900%.

- **<u>El estallido</u>:** En esta etapa es donde entraría la mayor polémica. En el caso de que efectivamente nos encontrásemos ante una burbuja financiera, ¿se podría considerar que la burbuja ha estallado ya? En ese caso, ¿cuánto le quedaría por bajar? Al tratarse de un activo principalmente usado en la actualidad con motivo de especulación, es imposible prevenir el comportamiento futuro que tendrá esta criptomoneda. (Noguera 2006)

Si diésemos por válida la suposición de algunos economistas de que esta "burbuja" ya ha explotado, no nos haría falta acudir a un análisis de las etapas de Minksy para ver que la cotización ha caído en picado. No es necesaria buscar la analogía de bitcoin con estas etapas para poder ver que la burbuja se estaría desinflando. En el último mes y medio previos al momento de redacción de este párrafo, el precio de Bitcoin ha alcanzado valores por debajo de la media registrada en las últimas doscientas jornadas acumulando una bajada del 58% desde sus máximos en diciembre de 2017. Esta caída en picado de la cotización podría identificarse con el fenómeno económico defendido por algunos economistas, conocido como el "cruce de la muerte"[li], siendo la definición de este el hecho de que se produzca en 50 días una caída de la cotización superando la media de las últimas 200 jornadas[lii]. Este podría ser uno de los indicadores de que la "burbuja especulativa de Bitcoin" hubiese podido explotar estos últimos meses.

Causas de Picos de subida y bajada de Bitcoin en el último año

En el gráfico expuesto en apartados anteriores expresando el aumento de recaudación de las ICO en los últimos años, el aumento de interés (sobretodo en 2017) hacia este tipo de criptodivisas es expuesto. Es a partir de 2014 donde la valoración de Bitcoin empieza a tener más peso puesto que los individuos conocen cada vez más de esta criptomoneda y se ven más interesados por ella.

Sin embargo, al igual que en los últimos años se han vivido las oscilaciones más representativas de esta criptomoneda, como podemos ver en el siguiente gráfico, ha sido este último 2017 y principios de 2018 los años en los que se han alcanzado los máximos y mínimos de la cotización de Bitcoin.

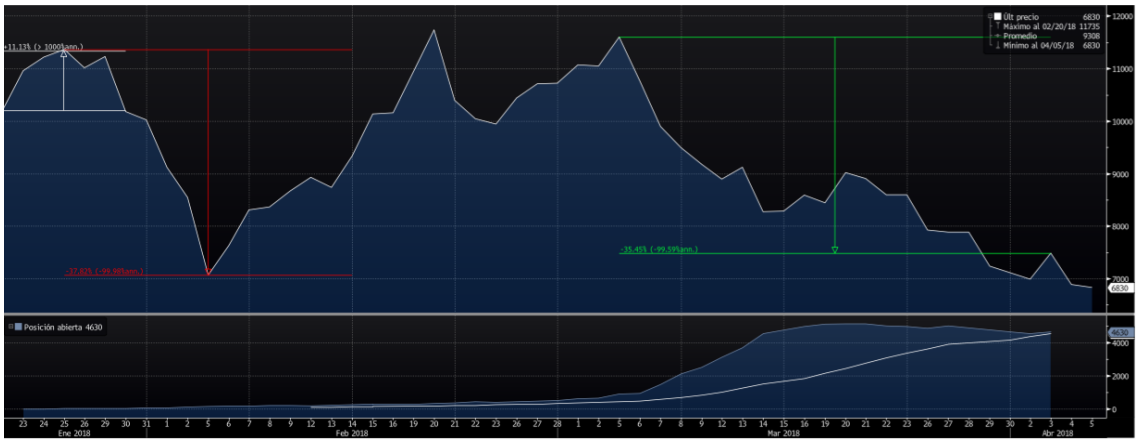
Gráfico 4: Histórico de cotización de Bitcoin

Fuente: Elaboración propia a través de plataforma de Bloomberg.

La principal razón por la que en diciembre de 2017 se alcanzó el máximo histórico de cotización (casi 20.000 dólares), es causa del lanzamiento de los futuros de Bitcoin de la Bolsa de Chicago (CBOE) que comenzó con una cotización superior a 15.400$. Esta oportunidad regulada y respaldada de invertir en Bitcoins produjo una compra masiva de criptomonedas que resultó en un aumento exponencial de la cotización.

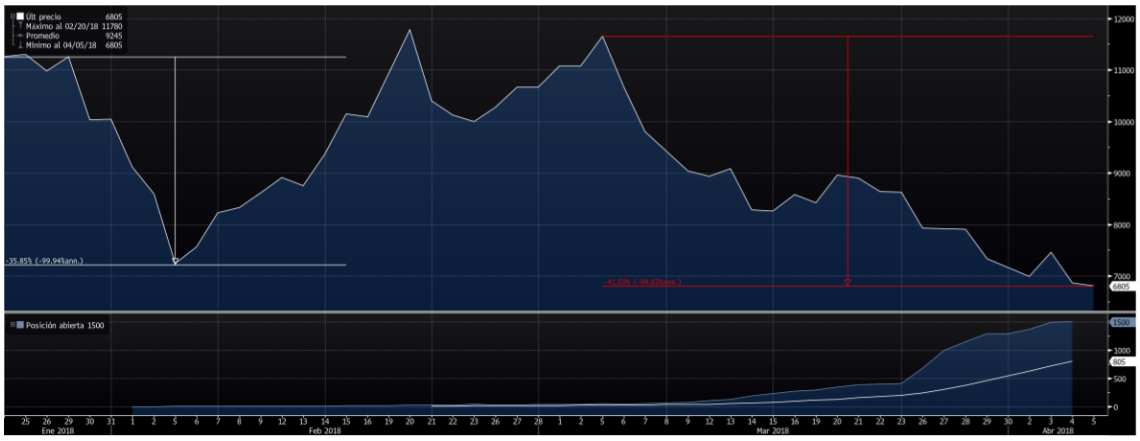
En los dos gráficos 5 y 6 expuestos a continuación, podemos observar en primer lugar la alta cotización de los futuros de la CBOE lanzados el 11 de diciembre seguida de la de los futuros de la CME lanzados 7 días después. A primera vista se podría decir que se trata del mismo gráfico, pero esto se debe a la cotización pareja y fecha de lanzamiento de ambos futuros.

Gráfico 5: Futuros de Bitcoin por la CBOE



Fuente: Elaboración propia a través de plataforma de Bloomberg.

Gráfico 6: Futuros de Bitcoin por la CME



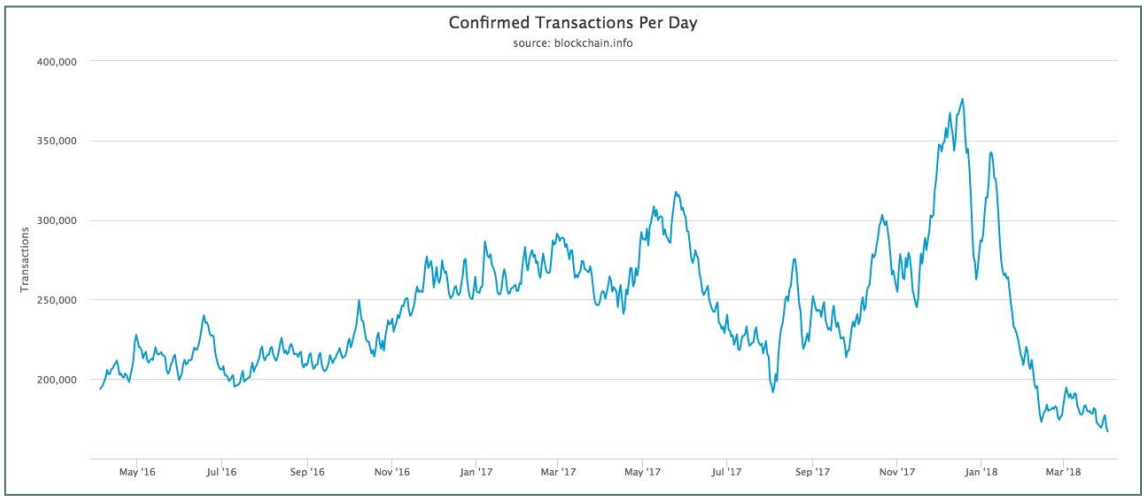
Fuente: Elaboración propia a través de plataforma de Bloomberg.

Sin embargo, tras su máximo histórico, Bitcoin de pronto empezó a caer tal y como podemos ver en los tres últimos gráficos estudiados tanto de futuros como en su cotización integral.

A pesar de que la principal causa de las oscilaciones de los precios de bitcoin puede ser la naturaleza deflacionaria de esta criptomoneda[liii], se ha podido observar que es ante la amenaza de una regulación inminente que el valor de la criptomoneda ha disminuido en más del 60% desde su máximo histórico[liv] que obtuvo en diciembre de 2017. La principal razón por la que se ha producido esta caída del valor de los bitcoins es la sensibilidad del valor de esta criptomoneda ante las noticias y creencias de los inversores. Las perspectivas de una regulación internacional de este tipo de divisas digitales provocaron una venta masiva, resultando en una caída en picado de la

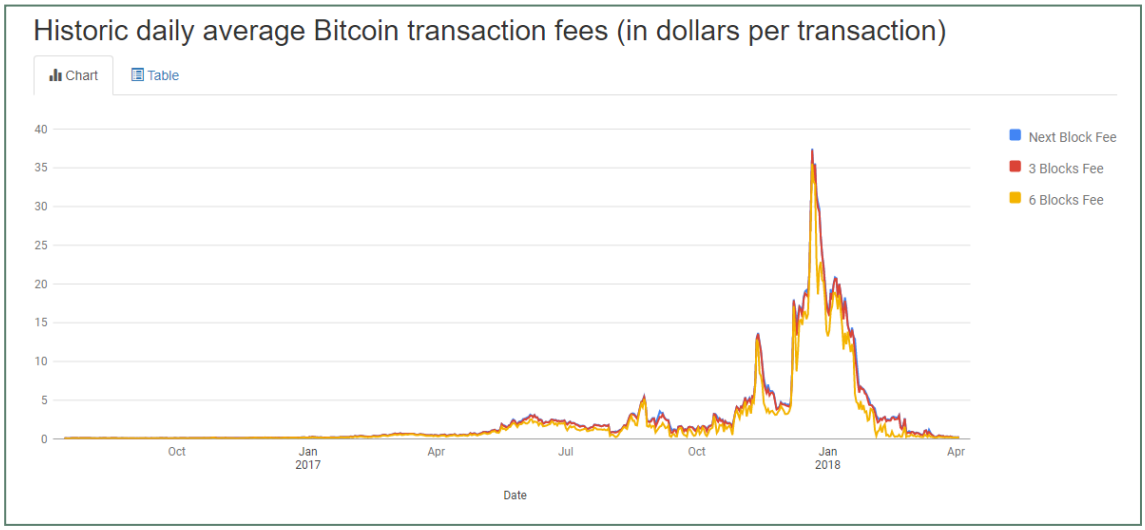
cotización. Asimismo, las "declaraciones de guerra" por parte de los grandes de internet como Google, provoca una falta de confianza sobre el futuro de la criptomoneda, lo que deriva en una caída del número de transacciones realizadas al día (ver primer gráfico expuesto a continuación) a pesar de que las comisiones por transacción han sido reducidas justamente para fomentar el número de transacciones realizadas (ver segundo gráfico expuesto a continuación).

Gráfico 7: Transacciones verificadas diarias



Fuente: Página Web Blockchain.info[lv]

Gráfico 8: Comisiones por transacción de Bitcoin a la semana



Fuente: Página Web BitcoinFees.info[lvi]

Sin embargo, a pesar de que la mayoría de los economistas defienden esta teoría de burbuja especulativa de Bitcoin, también destacan que en el caso de que esta burbuja

explotase, las repercusiones no serían significativas para la economía general a pesar de que este mercado de criptodivisas mueve miles de millones de euros y atañe a muchas personas alrededor del mundo. Esto se puede apreciar gracias a la web de CoinMarketCap [lvii] en la que en el momento de redacción de este párrafo, la capitalización de criptomonedas llegaba a $263.699.034.123, es decir 263 mil millones de dólares.

¿Y si no es una burbuja especulativa?

Si lo analizamos desde el otro punto de vista, se podría decir que cuanto más adoptada y usada este bitcoin en la economía, más se estabilizará. Tal y como nos explicaba Iñigo Molero:

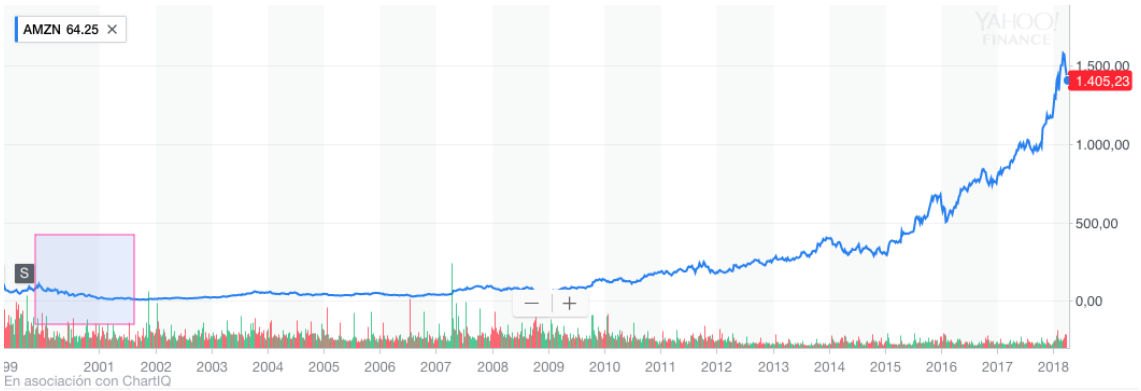
> *"Cuando el mercado sea más estable, cuando se hayan desarrollado más aplicaciones funcionales, que todo sea más práctico, sí que creo que tenderá a estabilizarse. Pero está claro que hoy en día la volatilidad es enorme"* (Molero 2018)

Tanto Blockchain como Bitcoin, llevan una tecnología detrás que todavía no ha podido ser entendida por la sociedad dada su complejidad y por encontrarse todavía en su fase embrionaria. Es por esto por lo que los inversores están apostando por esta criptomoneda simplemente por las altas rentabilidades que está teniendo últimamente, pero sin entender completamente los usos que se le puede dar a esta tecnología[lviii] y la importancia que podría tener en un futuro. Esto provoca una fuerte especulación, y consigue que en vez de darle un uso a Bitcoin como medio de pago rápido, eficiente, seguro y desligado de los bancos, simplemente se le está dando un uso especulativo.

Si comparamos a Bitcoin con otras grandes empresas tecnológicas que sufrieron la burbuja financiera de las puntocom como puede ser el caso de Amazon, podemos ver en el siguiente gráfico que esa crisis financiera, no tiene un gran peso en la histórica de su cotización por lo que no supuso un impedimento para que Amazon se convirtiese en el monstruo de internet que es hoy (el rectángulo que muestra la época de la burbuja

financiera de las puntocom). Podemos apreciar que es prácticamente imperceptible esta crisis dentro de la histórica de esta empresa.

Gráfico 9: Cotización Amazon desde las "puntocom"



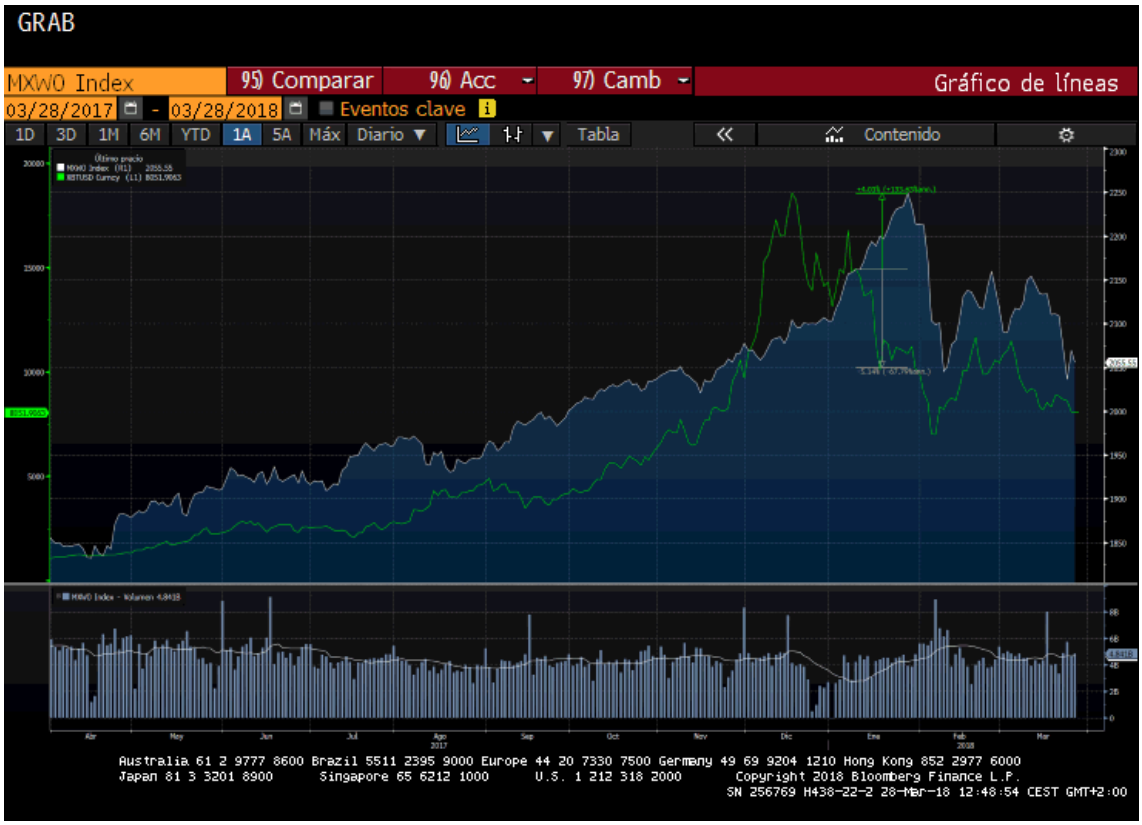
Fuente: Web Yahoo Finance [lix]

Con esto lo que queremos poner en evidencia, es que a pesar de que hoy por hoy la cotización de Bitcoin esté cayendo en picado por la posible regulación y se esté poniendo en entredicho la perpetuidad que podría tener esta criptomoneda, nadie nos puede decir con certeza que pueda convertirse en el futuro medio de pago internacional y que las deficiencias causadas por la especulación desaparezcan porque se llegue a estabilizar.

Correlación entre Bitcoin y el los principales índices del mercado.

En el siguiente gráfico podemos apreciar gracias a una comparación realizada entre el cruce del Bitcoin del dólar junto con el índice MSCI, como el valor de la criptomoneda no sigue las tendencias del mercado dado que son otros factores los que influyen en la cotización de este activo. En este caso, hemos elegido el uso del MSCI World Index para la comparativa dado que representa la capitalización de 1.653 empresas alrededor del mundo, y debido a la presencia distribuida internacional que tiene Bitcoin, ambas capitalizaciones cumplen esta característica.

Gráfico 10: Comparativa de Bitcoin con MSCI World Index



Fuente: Elaboración propia en plataforma de Bloomberg.

Estudios realizados por Chris Burniske y Jack Tatar demuestran han conseguido calcular una correlación casi cero entre Bitcoin y los principales índices usados a la hora de analizar opciones y bonos. Estos economistas aseguran con sus cálculos que añadiendo un uno por ciento de Bitcoin en una cartera que se compone un 30% de bonos y un 70% de acciones (siendo esta última categoría donde se incorporan los Bitcoin), produciría que el retorno de las carteras aumentase a costa de un moderado incremento de volatilidad (se incrementa su ratio de Sharpe). (Chris Burniske & Jack Tatar 2018). Esto se debe a que dada la baja volatilidad del mercado en los últimos tiempos y a la casi nula correlación de Bitcoin con este, con esta criptomoneda se puede aumentan las probabilidades de tener retorno en las carteras puesto que si no se gana en unas, es muy probable que se ganen con las criptomonedas.

Conclusión

Tras haber estudiado en profundidad tanto la condición tecnológica como la especulativa de estas criptomonedas, se podría decir que Bitcoin a la hora de ser observado desde el punto de vista de un inversor, está "envuelto en un papel de regalo" en forma de liberalismo y de tecno-misticismo que convierte a estas criptomonedas en un activo de inversión muy atractivo dados sus antecedentes de rentabilidad. Sin embargo esta falta de regulación por parte de los gobiernos y su alta volatilidad son duramente criticadas por la sociedad, principalmente por los inversores minoritarios que no entienden bien las funcionalidades que se le podría dar a estas criptomonedas y a su tecnología. En este informe hemos podido observar que las posibilidades que ofrece Bitcoin tanto con su Blockchain madre como con las sidechains que se están incorporando a su sistema son infinitas y que incluso el propio mercado de criptomonedas es en parte partidario de una regulación.

Los últimos niveles de cotización de Bitcoin muestran que tras una época de "montaña rusa" la cotización se está comenzando a estabilizar. Esto puede deberse a que aunque las previsiones del futuro de Bitcoin no sean muy prometedoras por parte de los analistas y economistas, Blockchain es la base en la cual realizan las transacciones de estas criptomonedas. La tecnología Blockchain gracias a la posibilidad de customización de las cadenas permite que sea utilizada en cualquier ámbito de la sociedad, optimizando así los procesos productivos y los modelos de negocio que conocemos actualmente, ofreciendo un nuevo internet del valor en el cual se puede realizar de forma anónima pero trazable transacciones internaciones de todo tipo, reduciendo los costes de transacción y el tiempo de ser validadas.

Hemos visto que tanto la condición de dinero de Bitcoin como el futuro de esta misma van a depender del volumen de aceptación que tenga en la sociedad, tal y como nos contaba Iñigo Molero:

"El éxito está en alcanzar un modelo de uso que sea global, y que llegue a la mayoría de la gente" (Molero 2018)

No queremos dar por terminado esta problemática sobre el futuro de esta nueva tecnología puesto que una respuesta absoluta no ha sido dada.
La vida recorrida por Bitcoin sigue siendo muy corta y al igual que los mayores cambios que ha tenido esta divisa digital han sido en el último año, nadie puede garantizar que el valor de Bitcoin no vaya a subir teniendo en cuenta que este no es el primer ciclo que vive esta criptomoneda.

Como conclusión, la precariedad de esta tecnología limita la visión de la sociedad, poniendo así límites a la investigación y evolución de este "nuevo sistema financiero". Hoy en día es poca la proporción de individuos en el mundo que le ven una verdadera funcionalidad a este nuevo internet del valor, pero cada vez son más los interesados y emprendedores en este mundo que es Blockchain y Bitcoin. Invitamos al lector a visualizar la charla impartida por el Digital Strategist Don Tapscott en las charlas Ted X[lx] en la cual se explican cinco funciones que ayudarían a la mejora de la globalización y de la economía.

Cabe preguntarse, ¿Hasta qué punto Blockchain va a ser incorporado en todos los aspectos de la sociedad? ¿Será capaz la sociedad de tirar a la basura lo que les han enseñado para abrazar este modelo descentralizado? ¿Ganará la especulación al verdadero valor intrínseco de Bitcoin?

BIBLIOGRAFÍA

Aleksandr Bulkin. 3 de Marzo de 2016. “Explaining blockchain-how proof of work enables trustless consensus” Keeping Stock. https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

Bima, Santiago. 2017. “Bitcoin: El coste del anonimato.” Trabajo de Fin de Master in Banking and Finance, Afi Escuela de Finanzas.

Burniske, Chris. 2018. Cryptoassets: The Innovative Investor’s Guide to Bitcoin and Beyond. U.S Jack Tatar.: McGraw-Hill Education.

“Diferencias entre las cadenas de bloques blockchain públicas y cadenas de bloques privadas” (2015) Oro y finanzas. https://www.oroyfinanzas.com/2015/10/diferencias-cadenas-bloques-blockchain-publicas-privadas/

Entrecanales Carrión, José. (Marzo 2014) “Burbujas Especulativas: Causas y Elementos Comunes”.

Fernando Naranjo. 26 de abril 2017. “El auténtico valor de Blockchain: su seguridad”. Expansión. http://www.expansion.com/economia-digital/protagonistas/2017/04/26/58dce9ede2704ea3378b4665.html

He, Dong, Ross Leckow, Vikram Haksar, Tommaso Mancini-, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Céline Rochon, and Hervé Tourpe. 2017. “Fintech and Financial Services: Initial Considerations.” Imf Wp, 49. https://www.imf.org/~/media/Files/Publications/SDN/2017/sdn1705.ashx.

Jayachandran, Praveen. 2017. “The difference between public and private blockchain” IBM Blockchain Blog. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Puschmann, T. (2017). Fintech. Business & Information Systems Engineering, 59(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Lewis, Antony. 2015. “Blockchain Technology Explained.” Blockchain Technologies, 1–27. doi:10.15358/0935-0381-2015-4-5-222.

Mecheba Molongua, Jessica. 2016. “Bitcoin, ¿la moneda del futuro?”.

Montes, Gabriel. Bitcoin Esencial: Claves sobre Claves privadas, públicas y direcciones. 30 de octubre de 2017. https://medium.com/@gab_montes/bitcoin-esencial-claves-sobre-claves-privadas-p%C3%BAblicas-y-direcciones-148f854b822d.

Molero, Iñigo. 2018. Interview by María Díaz de Bustamante Interview. In person. Madrid.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.” Www.Bitcoin.Org, 9. doi:10.1007/s10838-008-9062-0.

Noguera, Alberto. 2006. “Las siete etapas de la burbuja”
http://www.albertonoguera.com/2006/05/las-siete-etapas-de-la-burbuja.html

Pisa, Michael, and Matt Juden. 2017. “Blockchain and Economic Development : Hype vs. Reality.” Center for Global Development Polixy Paper (107), no. Center for Global Development Polixy Paper (107): 1–49.
https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

“¿Qué es una clave privada y pública, dirección y firma digital en Bitcoin?” (2016). Oro y finanzas. https://www.oroyfinanzas.com/2016/05/que-bitcoin-clave-privada-publica-direccion-firma-digital/

Rosic, Ameer. 2016 "What is Blockchain Technology? A step-by-step guide for beginners" Blockgeeks. https://blockgeeks.com/guides/what-is-blockchain-technology/

Sánchez de Diego, Jaime. 2014. Bitcoins. ¿Revolución o Historia?

Sanchis, José Luis. 2008. “Las 7 etapas de una burbuja financiera”.
https://www.rankia.com/blog/elinversorsosegado/431818-7-etapas-burbuja-financiera

Smith, Peter, and Candice Rosevear. 2017. “The Digital Revolution Bitcoin and The Future of Digital Assets.” Blockchain.
https://www.blockchain.com/assets/pdf/TheDigitalRevolution-Blockchain.pdf.

Yermack, David. 2015. “Is Bitcoin a Real Currency? An Economic Appraisal.” In Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, 31–43. Elsevier Inc. doi:10.1016/B978-0-12-802117-0.00002-3.

ANEXOS

Entrevista a Iñigo Molero, co autor del libro "Blockchain: La Revolución Industrial de Internet"

¿Qué futuro le ves a Blockchain y a las criptomonedas?

Le veo un futuro enorme. En el libro hablamos de eso. Creo que estamos ante una nueva tecnología que va a ser tan disruptiva como fue internet en su momento. Estamos pasando por las mismas etapas. Si te fijas los comentarios que se hacían en su día comparados con los de hoy son muy similares, "Esto es para pedófilos, terroristas, etc.".

Si perdiéramos internet de la noche a la mañana, perderíamos toda la fisionomía del planeta.

Si, internet ha sido algo maravilloso, pero tenía un problema en sí mismo.

Un ejemplo: si yo te mando una foto ese archivo se replica. Pues con Blockchain lo que consigue es que esa foto si yo te la quiero mandar, desaparezca de mi ordenador. Es decir que podamos transmitir valor a través de internet. Esto te abre un montón de campos en muchas industrias optimizándolas. Es una tecnología que ha llegado para quedarse, y que ahora mismo estamos en unos momentos muy incipientes, en una fase muy embrionaria. Incluso aún estamos haciendo el vocabulario, tenemos que ir dándole forma. En 3, 4, 5 años veremos cómo han cambiado muchos modelos de negocio y muchas relaciones sociales. Es tan transversal que puede estar desde en banca hasta en las redes sociales.

Según tú, ¿qué finalidad le dio Satoshi a esta tecnología cuando juntó todas aquellas ideas?

El objetivo principal, la idea general de Satoshi, era hacer un dinero digital. "Vamos a optimizar qué es el dinero"

El lanzamiento de Bitcoin coincide con 2009 la crisis. Cypherpunk es un movimiento muy libre, la tecnología a favor de los ciudadanos, etc. Entonces vamos a hacer un dinero soberano porque está siendo todo un cachondeo lo que ha ocurrido. Y si algo está claro es que Bitcoin ha venido para quedarse.

¿En qué se basa Blockchain para que no necesite un ente centralizado?

El éxito de una Blockchain se sustenta en tres patas:

- *Los desarrolladores: gente de inmenso talento que está continuamente trabajando para mejorar el código. Por ejemplo: RSK, una empresa argentina que en diciembre sacó un prototipo para sobre la Blockchain de bitcoin para hacer contratos inteligentes (como lo que hace Ethereum).*
- *La seguridad: los mineros. Bitcoin hoy por hoy es la Blockchain pública más segura del mundo. La capacidad de cómputo que tiene es abismal y si alguien quiere hackearlo tiene que meter una capacidad de cómputo que es imposible.*
- *La comunidad: la gente que soporta una criptomoneda. Bitcoin tiene una comunidad más beligerante, la primera de todas y la que más que cree en esto que estamos haciendo.*

¿No crees que hoy en día la gente se fija más en la especulación de Bitcoin más que en la tecnología que tiene detrás?

Es normal dada su etapa embrionaria. Pero yo esto lo veo como una ventaja. Porque si las personas ven en los medios de comunicación temas sobre Bitcoin o Blockchain, esto produce que más personas se sientan interesadas, investiguen y se vean cautivados por este tema. Pero todo eso cuando el mercado sea más estable, cuando se hayan desarrollado más aplicaciones funcionales, que todo sea más práctico, sí que creo que tenderá a estabilizarse. Pero está claro que hoy en día la volatilidad es enorme y hay que ser muy consciente de donde te estas metiendo. Esto no deja de ser un experimento. Podrías actuar como un holder para ver que va a pasar.

¿Crees posible una regulación comunitaria?

Los estados no saben cómo meterle mano a esto. Si te fijas los países más listos (los de siempre Suiza, Singapur, incluso Londres que después del Brexit está dando un subidón enorme que está intentando atraer talento para desarrollar esta tecnología) están invirtiendo en este tipo de tecnología.
Entonces hay varias posturas:

- *Los países que acabamos de mencionar que dicen: Esto va ser una revolución extraordinaria, las próximas grandes multinacionales van a estar sobre Blockchain. Vamos traer esta tecnología a nuestro país y así creamos riqueza y puestos de trabajo.*
- *Países que no saben muy bien que hacer como España que hará lo que decida la Unión Europea.*
- *Países como China que prohíben estas prácticas porque se les va de las manos. Los prohíben como forma de regularlo. Esta regulación es exigida también por los mercados de criptomonedas. Si se regula, imagínate todo el dinero institucional que puede venir al mundo de las criptomonedas. Hay muchas inversiones que por el momento están fuera porque estamos en un limbo jurídico que no se sabe muy bien como meterle mano. La regulación vendrá, lo que hay que hacer en España por ejemplo es que los reguladores tengan una postura abierta y positiva hacia este mercado y atraer esta tecnología al país.*

¿Entonces con la regulación habría que buscar ese equilibrio no?

Efectivamente. Lo que no se puede hacer es que para que gremios se mantengan, perder la oportunidad nosotros de desarrollar este tipo de tecnología. Tendría que haber una especie de ten con ten donde ambas partes ganen. Blockchain no deja de ser una forma de optimizar recursos y hacerlos mucho más baratos.
Pero todo esto está por ver, nadie te puede decir con certeza que es lo que va a pasar.

¿Qué posturas toman los bancos ante esta tecnología?
Bitcoin puso en evidencia para los bancos que su modelo de negocio, de la noche al día se podría ir al traste. (Ejemplo de ONGs que donde el banco se quedaba por cada euro con 80 céntimos de costes de transacción). Que las cantidades donadas llegaba prácticamente integras. El modelo de los bancos que utilizan tecnologías de hace décadas, es susceptible de ser mejorado. Las grandes empresas del IBEX están buscando también como quitarse a los bancos.
Se podría decir que los bancos han llevado a cabo las fases de negación que se la tribuyen a Gandhi:

- *Primero te ignoran: se hace caso omiso de esta tecnología diciendo que esto es de frikis.*
- *Segundo: Se ríen de ti*
- *Te combaten: Alegando "esto es de terroristas, burbuja especulativa, etc."*
- *Te ganan o se unen: intentan meter Blockchain en sus sistemas para optimizar sus propios procedimientos (teniendo que llevarse a cabo esto primero con una regulación).*

¿Crees que Bitcoin es una burbuja y que se ha desinflado?

Se irá estabilizando cuanta más adopción haya. Cuando nació Wall Street que el mercado era muy pequeño, la volatilidad también era muy alta. El valor subyacente que le veo a bitcoin, es que le veo una tecnología detrás. Si tu te fijas en las características del dinero: divisible, escaso y fácil de transportar, Bitcoin ha sido capaz de optimizar todas estas cosas.

	ORO	*FIAT*	*BTC*
Divisible	*no*	*si*	*si*
Escaso	*si*	*no*	*si*
Fácil de transportar	*no*	*si*	*si*

Mientras que la revolución tecnológica ha tenido repercusiones en casi todos los sectores, el dinero ha evolucionado muy poco, parecía que se había estancado.

¿En qué tipo de proyectos de Blockchain participas tú?

Ahora mismo estoy participando en varios. Uno de ellos es EthicHub.
Tenemos por un lado agricultores desbancarizados. Existen 2.000 millones de personas que están desbancarizadas, que no tienen dinero en los bancos. La mayoría de ellos son agricultores que tienen una actividad muy rentable (café, caña de azúcar). Pero como no tienen ese acceso a dinero para comprar semillas y demás, recurren a solicitar préstamos en su comunidad en efectivo. Y les cobran más de un 100% de intereses al

año. Nosotros proponemos crear un ecosistema donde todas las partes ganen ¿Cómo lo hacemos? Utilizando la tecnología Bk. Poniendo en contacto a individuos de Europa por ejemplo con recursos (aquí es donde entra romper las barreras del dinero), donde al guardar el dinero en el banco con los tipos impuestos actualmente no da ninguna rentabilidad, con los agricultores en necesidad de información. A través de bk eliminar a los intermediarios y mediante contratos inteligentes donde nosotros no tenemos nada que ver, tú les puedas prestar a estos 1000 euros por ejemplo, y ellos te devuelvan a ti un 15% de rentabilidad. Todo el mundo gana en este tipo de ecosistemas.

¿Qué implicaciones ha tenido Blockchain con respecto a la globalización?

Se han roto las fronteras del dinero.
China tiene unos controles muy estrictos de su divisa, mucho control, y Bitcoin rompe esos controles permitiendo la fuga de capitales. Pero sin embargo, con bitcoin tienes que tributar por las plusvalías, el % que has ganado, a no ser que no lo cambias por dinero fiat. Esto es más líquido que una acción de telefónica ahora, con la fórmula que ellos llaman HashCash. Incluso un domingo puedes liquidar tus criptomonedas, cosa que con una acción de telefónica no podrías. Te mandan un código a tu móvil a la App, la introduces en un cajero y puedes sacar en efectivo tus bitcoins en ese cajero. El Banco Popular ofrece ese servicio. Hay una aplicación que es Bit2me que te indica en que cajeros puedes sacar tus criptomonedas en efectivo. Esto funciona ininterrumpidamente 24 horas, 7 días a la semana durante todo el año, y en todo el mundo porque es global.

¿Blockchain rompe todos los paradigmas de la distribución económica actual?

Te pongo un ejemplo: Imagínate que una pequeña empresa nativa de Blockchain va a poder combatir con las grandes multinacionales. Imagínate un barco que va a realizar una travesía con toneladas de mercancía. Este barco quiere contratar un seguro que en caso de hundimiento le pague 100 millones de euros, pagando para ello una prima de 5 millones de euros. Una pequeña empresa Insurtech, que sean 8 o 10 tíos, muy nativos en Blockchain, pueden emitir 100 millones de criptomonedas y las vendo a 1 euro cada uno. Cojo 100 millones de euros, los meto en un banco a expensas de lo que ocurra con el barco. La travesía es de 3 semanas. Si el banco se hunde, los 100 millones van al

barco, las criptomonedas valen cero, has perdido tu inversión. Pero si el barco llega al final, esos 5 millones de euros van a las criptomonedas, y tú al final has ganado un 5% en 3 semanas. O sea estos negocios que estaban muy ligados a las grandes compañías de seguros que sí que podían tener a disposición esos 100 millones, pues ahora lo puede asumir una pequeña compañía y poner a disposición de los demás que quieran invertir en esto. Cualquiera de nosotros vamos a poder participar en este tipo de negocios. Democratizas el acceso.

¿Crees de verdad que Bitcoin es una inversión segura?

Bitcoin sí que me da mucha seguridad, y yo creo que ya hemos pasado esos momentos más duros. Cuanta más gente lo entiende, más se incorpora. No hubiesen sacado futuros si no hubiesen visto que hay oportunidad de negocio. Y también me gusta mucho otra cosa de los futuros, que aún no lo veremos. En el mercado de la plata, para que nos hagamos una idea, con los futuros y todas las clases de inversión, se comercializa al día con más plata de la producción anual. Los futuros empezaron con una idea buena al principio, para estabilizar el precio de los mercados, pero como todo en esta vida se ha industrializado y se ha ido de madre. Que en un día tu negocies más plata de la que existe, no tiene sentido.

¿Estás de acuerdo con que la imagen de Satoshi Nakamoto sea anónima?

El éxito de las organizaciones descentralizadas, es que el propio catalizador, el fundador, en un momento dado lo monte y se vaya y que la propia estructura sigue por si sola. Hasta en esto Bitcoin es perfecto, porque en Ethereum, si mañana le pasa algo al fundador, la cotización bajaría y se pondría en entredicho que continúe. Satoshi Nakamoto en 2011 desapareció y dejo a la comunidad que se mantuviese sola para no depender de nadie.

Para ti, ¿qué es lo más drástico a lo que se le puede hacer un uso de Blockchain?

La democracia líquida. Que tu voto fuera un token. Fíjate que idea más maravillosa: el Partido A se presenta. Mi voto es un token, vemos todos cuantos votos ha recibido y no se puede falsear. Luego vemos que no cumple sus promesas, le quitamos el token y lo llevamos a otro partido. Y por ejemplo si el cambio supera al 40% se convocan elecciones inmediatamente. Esto obligaría a los políticos a cumplir sus promesas y que todos tuviéramos una encuesta real del día a día de los partidos políticos. Esto crearía una democracia de verdad, y la haría madurar mucho más. Seriamos ciudadanos en todo el sentido, con un completo derecho de voto.

"Lo más fascinante de este mundo, es que el único límite es nuestra propia capacidad de imaginar posibilidades"

"El éxito está en alcanzar un modelo de uso que sea global, y que llegue a la mayoría de la gente"

En caso de que no se llegase a una regulación comunitaria, ¿qué piensas de que los países les cierren las puertas a esta tecnología?

No se puede poner puertas al campo. En el caso de que no se pueda hacer uso de esta tecnología en un país, entonces el talento y las inversiones se irán donde lo hayan reconocido la importancia Mi esperanza es que en un futuro todos los países se igualen por arriba y que sea una cuestión de quien es el más permisivo con el desarrollo de la tecnología.

"15 días en un ecosistema es como un año en cualquier industria centralizada.
Yo ya tengo problemas para seguir la actualidad de este mercado"

Después de cómo ha bajado la cotización, ¿Sigues pensando que Bitcoin es una buena inversión?

Mientras que en el internet de la información, todas las grandes empresas como Amazon o Google, comparten el mismo protocolo (TFP, IP) que es el protocolo sobre el que sustenta todo internet. Pero nadie sustenta este protocolo, nadie se retribuye por el hecho de haber creado algo que se usa diariamente en el mundo entero.
Pero en el caso de Bitcoin, ocurre exactamente lo contrario. Aquí puede ser bitcoin, u otra. Las industrias se van a construir sobre estos protocolos, cuanto mayor sea el valor que alcanzan estas empresas, mayor va a ser el valor de estos protocolos que la sustenten.

Bitcoin poco a poco va teniendo más oportunidades gracias a los sidechain, como es el caso de RSK que hace lo mismo que Ethereum pero dentro de la plataforma de Bitcoin.
Además han implementado otras cosas muy interesantes. Aquí parte de los mineros, parte de lo que utilizan para minar bitcoin, lo van a utilizar para ejecutar esos Smart contracts por lo que les están optimizando a los mineros.

Todo empezó en bitcoin, y ahí sigue, siendo la principal después de 9 años.

¿Cómo implementarías tú esta tecnología en las instituciones públicas?

Una de las quejas de los autónomos es que tienen que hacer ellos mismos las declaraciones de hacienda. Pero a través de Blockchain, las facturas se devengarían inmediatamente a Hacienda por lo que se disminuiría la economía sumergida. Automáticamente con los Smart contracts, las declaraciones van a una dirección con el hash y con todo. Todo estaría en esa base de datos donde todos podríamos acceder.
También se podría vigilar el recorrido que hacen las subvenciones.
Necesariamente Blockchain va a fomentar las buenas prácticas por tener temor a que te pillen. Todos nosotros podremos hacer ese seguimiento, y se crearan puestos de trabajo también.

¿En una Blockchain Privada puedes poner las condiciones que quieras?

Las Blockchain privadas son como un Audi. El motor y la carrocería tiene que ser de la marca, pero luego el color y los asientos los puedes elegir tú, pero no deja de ser un Audi. Pasa lo mismo con las Blockchain Privadas. Al final tu puedes diseñar una con las características que tú quieras y el en futuro se podrá encontrar una unión para que las diferentes Blockchain puedan operar entre ellas.

BIBLIOGRAFÍA WEB

[i] Coindesk. "How Does Blockchain Technology Work?" Consultada 6 de febrero, 2018. https://www.coindesk.com/information/how-does-blockchain-technology-work/

[ii]Nocreasnada."¿Cómo Funciona Blockchain? La Guía Definitiva – Nocreasnada." Consultada 6 de febrero, 2018. https://www.nocreasnada.com/como-funciona-blockchain/

[iii]Blockchain.Com."Whitepaper Blockchain." Consultada 7 de febrero, 2018. https://www.blockchain.com/whitepaper/index.html

[iv]Bitcoin.Org. "How Does Bitcoin Work? – Bitcoin." Consultada 10 de febrero, 2018. https://bitcoin.org/en/how-it-works

[v] Blockchain.Info. "Bitcoin Block #517051". Consultada el 22 de febrero, 2018. https://blockchain.info/block/000000000000000000044b81c0c0b7fa47e194239f291726f5ef5c70cb58fffea

[vi]Oroyfinanzas.Com. "Cadenas De Bloques (Blockchain) Públicas Vs Privadas". Consultada 26 de febrero, 2018. https://www.oroyfinanzas.com/2015/10/diferencias-cadenas-bloques-blockchain-publicas-privadas/

[vii]Floyd, David. 2018. "How Bitcoin Works". Investopedia. https://www.investopedia.com/news/how-bitcoin-works/

[viii]Pastor, Javier. 2018. "Monederos Físicos De Bitcoin: Qué Son Y Cómo Funcionan A La Hora De Proteger Tus Inversiones". Xataka.Com. Consultada 22 de febrero, 2018. https://www.xataka.com/criptomonedas/monederos-fisicos-de-bitcoin-que-son-y-como-funcionan-a-la-hora-de-proteger-tus-inversiones

[ix]Bitcoin.Org. "How Does Bitcoin Work? – Bitcoin." Consultada 10 de febrero, 2018. https://bitcoin.org/en/how-it-works

[x]Blockchain.Info. "Bitcoin Transaction 1E190a3c045d8404aae82a98f1104e9ba1ff2027f6a48fcca1078cb0e2cb079a." Consultada 2 de marzo, 2018. https://blockchain.info/tx-index/252890411?show_adv=true

[xi]Oroyfinanzas.Com. "¿Qué Es Una Clave O Dirección Privada Y Pública En Bitcoin?". Consultada 2 de marzo, 2018. https://www.oroyfinanzas.com/2016/05/que-bitcoin-clave-privada-publica-direccion-firma-digital/

[xii]Medium. "Bitcoin Esencial: Claves Sobre Claves Privadas, Públicas Y Direcciones". Consultada 3 de marzo, 2018. 148f854b822d. https://medium.com/@gab_montes/bitcoin-esencial-claves-sobre-claves-privadas-p%C3%BAblicas-y-direcciones-148f854b822d

[xiii]Bit2me • El Blog De Bitcoin. "Transacciones Bitcoin, ¿Cómo Funcionan?". Consultada 3 de marzo, 2018. https://blog.bit2me.com/es/transacciones-bitcoin/

[xiv] Bit2me • El Blog De Bitcoin. "Transacciones Bitcoin, ¿Cómo Funcionan?". Consultada 3 de marzo, 2018. https://blog.bit2me.com/es/transacciones-bitcoin/

[xv] Bitcoin.Org. "Some Things You Need To Know - Bitcoin". Consultada 4 de marzo, 2018. https://bitcoin.org/en/you-need-to-know

[xvi] Chainalysis.com."Chainalysis - Blockchain Analysis". Chainalysis. Consultada 4 de marzo, 2018. https://www.chainalysis.com/

[xvii] Oroyfinanzas.Com. "¿Qué Es Un Halving En Bitcoin?". Consultada 4 de marzo, 2018. https://www.oroyfinanzas.com/2015/09/que-es-halving-bitcoin/

[xviii]Hashcash.Org. "Hashcash And Bitcoin". Consultada 7 de marzo, 2018. http://www.hashcash.org/bitcoin/

[xix] Thebookofbitcoin.Github.Io. "The Book Of Bitcoin". Consultada 7 de marzo, 2018. https://thebookofbitcoin.github.io/html/mining/hashcash.html

[xx] Crytomusing. "Mining". Consultada 9 de marzo, 2018. http://www.cryptomusing.com/mining.html

[xxi] Tar, Andrew. 2018. "Proof-of-work, Explained." Cointelegraph.Com. Consultada 10 de marzo, 2018. https://cointelegraph.com/explained/proof-of-work-explained

[xxii] Libro Blockchain. 2018. "Hashcash - Libro Blockchain". Consultada 10 de marzo, 2018. http://libroblockchain.com/hashcash/

[xxiii]Coindesk. "Bitcoin Hash Functions Explained – Coindesk". Consultada 11 de marzo, 2018. https://www.coindesk.com/bitcoin-hash-functions-explained/

[xxiv]Crytomusing. "ICO's". Consultada 12 de marzo, 2018. http://www.cryptomusing.com/icos.html

[xxv] Momoh, Osi. 2018. "Initial Coin Offering (ICO)". Investopedia. Consultada 12 de marzo, 2018. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

[xxvi]Cointelegraph.Com. "Falsas ICO, estafas comunes de criptos y cómo evitarlas." Consultada 13 de marzo, 2018. https://es.cointelegraph.com/news/fake-icos-common-crypto-scams-and-how-to-avoid-them

[xxvii] Elementus.io. "Four Years Of Initial Coin Offerings, Visualized In One Graphic". Consultada 25 de marzo, 2018. https://elementus.io/token-sales-history

[xxviii] Tecnobits.Xyz. "Los 5 Mejores Exchanges Para Trading De Criptomonedas (2018)". Consultada 25 de marzo, 2018. http://tecnobits.xyz/mejores-exchanges-para-trading-de-criptomonedas-2018/

[xxix] Crytomusing. "Wallets". Consultada 25 de marzo, 2018. http://www.cryptomusing.com/wallets.html

[xxx] Pastor, Javier. 2018. "Monederos Físicos De Bitcoin: Qué Son Y Cómo Funcionan A La Hora De Proteger Tus Inversiones". Xataka.Com. Consultada 22 de febrero, 2018. https://www.xataka.com/criptomonedas/monederos-fisicos-de-bitcoin-que-son-y-como-funcionan-a-la-hora-de-proteger-tus-inversiones

[xxxi] Coindesk. "How To Store Your Bitcoins - Bitcoin Wallets - Coindesk". Consultada 15 de marzo, 2018. https://www.coindesk.com/information/how-to-store-your-bitcoins/

[xxxii] Igartua, María. 2018. "Europa Quiere Regular Bitcoin Mientras La Criptomoneda Tiene Ya Los 20.000 A Tiro. Noticias De Mercados". El Confidencial. Consultada 20 de marzo, 2018. https://www.elconfidencial.com/mercados/2017-12-18/regulacion-bitcoin-riesgos-terrorismo-blanqueo-drogas_1494672/

[xxxiii] Forbes.Com. "Bitcoin cryotocurrency and the government regulation paradox". Consultada 18 de marzo, 2018. https://www.forbes.com/sites/jayadkisson/2018/01/29/bitcoin-cryptocurrency-and-the-government-regulation-paradox/2/#6071d4602fae

[xxxiv] Velasquez, Germey. 2018. "Solo 807 Personas Declararon Por Impuestos Bitcoin Ante El IRS De EE.UU – Infocoin". Infocoin.Net. Consultada 19 de marzo, 2018. http://infocoin.net/2017/03/22/solo-807-personas-declararon-por-impuestos-bitcoin-ante-el-irs-de-ee-uu/

[xxxv] CoinTelegraph. "China after banning exchanges authorities move to clase Exchange like services". Consultada 19 de marzo, 2018. https://es.cointelegraph.com/news/china-after-banning-exchanges-authorities-move-to-close-exchange-like-services

[xxxvi] Foro.Coinmarketcap.Store. "Google Declara La Guerra A Las Criptomonedas - Foro De Coinmarketcap". Consultada 1 de abril, 2018. http://www.foro.coinmarketcap.store/viewtopic.php?f=3&p=52

[xxxvii] CoinTelegraph. "Bitcoin regulation is simple in theory, incredibly complex in reality." Consultada 19 de marzo, 2018 https://es.cointelegraph.com/news/bitcoin-regulation-is-simple-in-theory-incredibly-complex-in-reality

[xxxviii] Analistas Financieros Internacionales, Afi. 2018. "Revista Empresa Global AFI". Empresaglobal.Es. consultada 20 de marzo, 2018. http://www.empresaglobal.es/EGAFI/contenido/1741693/1601149/la-cara-oculta-de-las-criptodivisas.html

[xxxix] Bank & rarr;, Ver. 2018. "Ripple, La Criptomoneda De Los Bancos". El Blog De Self Bank. Consultada 20 de marzo, 2018. https://blog.selfbank.es/ripple-la-criptomoneda-de-los-bancos/

[xl] De Haro, José Luis. 2017. "El bitcoin supera ya a los tulipanes como la burbuja más grande de la historia." El Economista. Consultada 7 de marzo, 2018. http://www.eleconomista.es/divisas/noticias/8805544/12/17/El-bitcoin-supera-ya-a-los-tulipanes-como-la-burbuja-mas-grande-de-la-historia.html

[xli] Macrotrends.Net. "Federal Funds Rate - 62 Year Historical Chart". Consultada 21 de marzo, 2018. http://www.macrotrends.net/2015/fed-funds-rate-historical-chart

[xlii] Tradingeconomics.com. "Euro Area Interest Rate". Consultada 21 de marzo, 2018. https://tradingeconomics.com/euro-area/interest-rate

[xliii] Macrotrends.Net. "Federal Funds Rate - 62 Year Historical Chart". Consultada 21 de marzo, 2018. http://www.macrotrends.net/2015/fed-funds-rate-historical-chart

[xliv] Tradingeconomics.com. "Euro Area Interest Rate". Consultada 21 de marzo, 2018. https://tradingeconomics.com/euro-area/interest-rate

[xlv] Domm, Patti. 2018. "Bitcoin is already dwarfing some of the largest financial market bubbles of all time". CNBC. Consultada 22 de marzo, 2018. https://www.cnbc.com/2017/11/30/bitcoin-dwarfing-some-of-the-largest-market-bubbles-of-all-time.html

[xlvi] Albertonoguera.com. "Las siete etapas de la burbuja". Consultada 28 de marzo, 2018. http://www.albertonoguera.com/2006/05/las-siete-etapas-de-la-burbuja.html

[xlvii] Coinbase.com. "Bitcoin, Ethereum, and Litecoin Price". Consultada 29 de marzo, 2018. https://www.coinbase.com/charts?utm_source=google_search_b&utm_medium=cpc&utm_campaign=1167028680&utm_content=51504596765&utm_term=%2Bcoinbase&utm_creative=257480424609&cb_device=c&cb_placement=&cb_country=es&cb_city=open&cb_language=en_gb&gclid=Cj0KCQjwnqzWBRC_ARIsABSMVTMk3eRxtegOETFzpJFMD8JsfMIm8Ov0jRbf8tmRi0tHJh61cCCNLjYaAoMgEALw_wcB

[xlviii] Vlastelica, Ryan. 2018. "Why bitcoin is now the biggest bubble in history, in one chart". MarketWatch. Consultada 28 de marzo, 2018.

https://www.marketwatch.com/story/why-bitcoin-is-now-the-biggest-bubble-in-history-in-one-chart-2017-12-13

[xlix] En Bolsa. "“Tonto el último: Identificando burbujas financieras” - En Bolsa". Consultada 15 de marzo, 2018. https://www.enbolsa.net/tonto-el-ultimo-identificando-burbujas-financieras/

[l] Coinmarketcap.com. "Bitcoin (BTC) price, charts, market cap, and other metrics | CoinMarketCap". Consultada 5 de abril, 2018. https://coinmarketcap.com/currencies/bitcoin/

[li] El Economista. “El cruce de la muerte amenaza con hundir el bitcoin hasta 2.800 dólares”. Consultada 4 de abril, 2018. http://www.eleconomista.es/divisas/noticias/9009693/03/18/El-cruce-de-la-muerte-amenaza-con-hundir-bitcoin-hasta-los-2800-dolares.html

[lii] ESTRATEGIAS DE TRADING. "Cruce de medias móviles: cruce de la muerte vs cruce dorado". Consultada 4 de abril, 2018. https://estrategiastrading.com/cruce-de-medias-moviles/

[liii]CoinTelegraph. “Regulations and their influences on cryptocurrency prices”. Consultada 29 de marzo, 2018. https://es.cointelegraph.com/news/regulations-and-their-influence-on-cryptocurrency-prices

[liv] Buybitcoinworldwide.com. "Gráfico de historial del precio de Bitcoin (Desde 2009)". Consultada 06 de abrtil, 2018. https://www.buybitcoinworldwide.com/es/precio/

[lv] Blockchain.info. "Confirmed Transactions Per Day". Consultada 07 de abril, 2018. https://blockchain.info/charts/n-transactions

[lvi] Bitcoinfees.info. "Bitcoin Transaction Fees". Consultada 1 de abril, 2018. https://bitcoinfees.info/

[lvii] Coinmarketcap.com. "Cryptocurrency Market Capitalizations | CoinMarketCap". Consultada 7 de abril 2018. https://coinmarketcap.com/

[lviii] Tiempo, Casa. 2018. "Este es el perfil de quienes le apuestan al bitcoin". Consultada 5 de abril, 2018. Portafolio.co. http://www.portafolio.co/economia/finanzas/conozca-el-perfil-de-las-personas-que-invierten-en-bitcoin-513600

[lix] Es.finance.yahoo.com. "Gráfico de cotización interactivo de AMZN | Acciones de Amazon.com, Inc. - Yahoo Finanzas". Consultada 7 de abril, 2018. https://es.finance.yahoo.com/chart/AMZN

[lx] Tapscott, Don. 2018. "How the blockchain is changing money and business". Ted.com. Consultada 7 de abril, 2018. https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business