MÁSTER OFICIAL EN EMPRESAS Y TECNOLOGÍAS DE LA INFORMACIÓN

2015/2016

TRABAJO FIN DE MÁSTER

CRIPTODIVISAS Y PAGOS ONLINE

CRYPTOCURRENCY AND ONLINE PAYMENTS

Autor

D. JAVIER A. CUARTAS MICIECES

Director

D. FRANCISCO JAVIER LENA ACEBO

7 Julio 2016

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer por su labor al coordinador y a todos los profesores del máster en Empresas y Tecnologías de la Información, en cuyo marco se ha elaborado éste Trabajo Fin de Máster y en especial, por su colaboración en la elaboración a D. Joaquín Cayón de las Cuevas, a quién se consultó en referencia a los aspectos regulatorios de las criptomonedas y a D. Francisco Javier Lena Acebo, por su ayuda como director del Trabajo.

Por otro lado, quisiera expresar mi agradecimiento al FABLAB de Santander y en especial a D. Constantin-Claudiu Tanasescu, por los talleres de bitcoin, que resultaron de mucha ayuda en el desarrollo del Trabajo y por su labor para incentivar el progreso de su entorno.

Para terminar, agradecer a mis padres y a mi familia su apoyo incondicional a lo largo de toda mi trayectoria.

ÍNDICE

1. INTRODUCCIÓN (pág. 6)

2. CONCEPTO Y ORÍGENES DE LAS CRIPTOMONEDAS (pág. 7-9)

2.1. Concepto de criptomoneda (pág. 7-8)

2.2. Historia y origen de las criptomonedas (pág. 8-9)

3. FUNCIONAMIENTO Y FUNDAMENTOS CRIPTOGRÁFICOS BÁSICOS (pág. 10-24)

3.1. Fundamentos técnicos y criptográficos básicos (pág. 10-13)

3.1.1 Firma digital (pág. 10)

3.1.2 Hash (pág. 10-11)

3.1.3 Merkle Trees e integridad entre nodos (pág. 11-12)

3.1.4 Blockchain como base de datos distribuida (pág. 13)

3.2 Proof of Work (bitcoin) (pág. 13-17)

3.3 Proof of Stake (Peercoin) y sus posibilidades como extensión de Proof of Work (pág. 17-19)

3.4 Bizantine Agreement (Ripple) (pág. 19-21)

3.5 Otras aplicaciones detrás de los fundamentos tecnológicos de las criptodivisas (blockchain) (pág. 21-24)

4. ECONOMÍA Y MERCADO DE LAS CRIPTOMONEDAS (pág. 25-42)

4.1. Índices y parámetros a utilizar en el análisis de las criptodivisas como inversión o medio de pago (pág. 25-26)

4.2. Factores de influencia a nivel general y específico respecto de otros medios de pago y de la moneda fiat (pág. 27-41)

4.2.1. Tecnología: impacto en el aspecto económico de las criptodivisas (pág. 27-30)

4.2.3. Economía y alcance: Postura de bancos y otras empresas y recomendaciones para la actividad comercial con criptodivisas (pág. 30-36)

4.2.2. Ecosistema: funcionamiento, aplicaciones y agentes (pág. 37-39)

4.2.4. Regulación en el mundo y en España (pág. 39-41)

4.4. Posibles escenarios futuros de la criptomoneda (pág. 41-42)

5. CASOS DE ESTUDIO (pág. 43-45)

5.1. Diseño de las entrevistas (pág. 43-44)

5.2. Conclusiones del estudio (pág. 44-45)

6. VENTAJAS E INCONVENIENTES: APLICACIONES E INTERÉS EN LA ESTRATEGIA DE LA EMPRESA (pág. 46-49)

6.1. Ventajas e inconvenientes frente a sus alternativas (pág. 46-47)

6.2. Integración en la estrategia de las empresas y posibilidades como fuentes de ventajas competitivas (pág. 47-49)

7. CONCLUSIONES (pág. 50-51)

8. PROPUESTAS DE MEJORA (pág. 52)

9. ANEJO I: FORMATOS DE ENCUESTA (pág. 53-54)

10. ANEJO II: RESPUESTAS (pág. 55-61)

11. BIBLIOGRAFÍA (pág. 62-66)

RESUMEN

Es la fuerte base de los conceptos criptográficos en los que se apoya la seguridad del bitcoin y las criptomonedas, la que ha hecho que se mantengan activas una gran variedad de las mismas a pesar de su volatilidad.

La comunidad de bitcoin debe enfrentarse aún a algunos problemas técnicos, además de la volatilidad del bitcoin y su falta de regulación, pero sigue siendo la criptomoneda más importante en el mercado.

La seguridad y privacidad que brinda su tecnología, así como la oportunidad de evitar los intermediarios en las transacciones económicas son las ventajas más relevantes que ofrece el bitcoin al mundo de los negocios. De hecho, los ahorros en transacciones internacionales han hecho que algunos bancos como el Fidor Bank de Alemania implementen éste tipo de tecnologías para ofrecer algunos servicios, y algunos negocios han declarado que éstos ahorros en pagos internacionales son el motivo de su aceptación de criptodivisas.

Al principio era más difícil que ahora, para un usuario común, ejecutar pagos seguros a través de bitcoin y había muchas estafas en el seno de su ecosistema. A pesar de ello, el entorno del bitcoin ha evolucionado para proveer mejores servicios en términos de confianza y facilidad de uso. Se espera del resto de las criptodivisas que sigan una evolución similar, en caso de que ganen la suficiente popularidad.

Hoy en día, podemos encontrar muchas tiendas online que aceptan pagos en criptomonedas, pero también hay empresas que nos facilitan opciones para pagar productos de tiendas que no aceptan éste tipo de pagos, como tarjetas de dédito recargables con criptodivisas.

Otro punto a tener en cuenta es la emergencia de negocios de tipo financiero en torno a las distintas criptodivisas y su dependencia de las empresas y profesionales de IT, en cuanto a oportunidades de empleo e inversión.

Además, el bitcoin nos ha traído el concepto de blockchain, que está siendo desarrollado y aplicado en un gran número de campos como la propiedad intelectual y la eficiencia energética. Las entidades financieras están estudiando esta idea con el fin de mejorar sus transacciones y enfrentarse con el éxito del bitcoin.

El objetivo de éste trabajo es analizar el concepto de criptomonedas, los factores que influencian su éxito y sus posibilidades en el mundo de los negocios.

Palabras clave: criptomonedas, criptodivisas, bitcoin, métodos de pago online, blockchain, internet

ABSTRACT

It is the strong foundation of the cryptographic concepts in which the security of cryptocurrencies and bitcoin rely on, that has led to a wide range of cryptocurrencies which is remaining active, despite its volatility.

Bitcoin's comunity is yet to face some technical problems, apart from bitcoin's volatility and its lack of regulation but it keeps being the most important cryptocurrency in the market.

The security and privacy which is brought by its technology, as well as the chance of cutting out the middlemen in economic transactions, are the most important advantages which bitcoin has brought to the business industry. In fact, savings on international transactions have driven some Banks, such as Fidor Bank of Germany, to implement this kind of technologies for providing some services, and some businesses have declared that these savings on international payments are the main reason why they accept cryptocurrencies.

In the beginning, it was much more difficult than now for a common user to securely carry out bitcoin payments and there were plenty of scams within this cryptocurrency ecosystem. Even so, bitcoin's environment has evolved to provide a better set of resources in terms of reliability and easy use. The rest of cryptocurrencies are expected to follow the same evolution as long as they gain enough popularity.

Nowadays, we can find many online retailers which accept cryptocurrencies but there are also some enterprises which provides us with options to pay in bitcoin any product from stores which doesn't accept this payment method, such as debit cards which can be reloaded with cryptocurrencies.

Another point to consider is the emergence of new financial businesses around cryptocurrencies such as exchanges, miners or payment processors, and its dependance on the activity of IT companies and professionals, as regards new investment and employment oppotunities.

On top of that, it is the bitcoin's idea that has brought us the concept of blockchain, which is being developed and applied in a large number of fields such as intelectual property or energy efficiency. Financial institutions are looking into this idea to improve its transactions and to deal with the bitcoin's success.

The aim of this work is to analyse the concept of cryptocurrencies, the factors which influence their success, and their possibilities in the world of business.

Keywords: cryptocurrency, bitcoin, online payment methods, blockchain, internet.

1. INTRODUCCIÓN

Éste Trabajo Fin de Máster pretende explorar el concepto de criptodivisa como innovación de reciente aparición, que ha logrado trascender con el tiempo las dificultades que acompañan a la descentralización como principio, convirtiéndose en un importante elemento en las transacciones comerciales online, a pesar de su escasa implantación, por las ventajas económicas y comerciales que entraña su uso a día de hoy.

Así, el redactor de éste trabajo, en un principio totalmente ignorante de su funcionamiento y consecuencias en el entorno, ha tratado, para su realización, de adquirir un adecuado entendimiento de los mismos, tratando de orientar el texto desde una explicación descriptiva de la historia, tecnología y condicionantes del objeto de estudio, hacia el interés que representa su adopción para la empresa y la sociedad, como último objetivo, tomando como partida la información bibliográfica referenciada, consultas a expertos sobre el tema, así como encuestas a empresas.

De éste modo, se ha partido de la explicación del concepto de criptomoneda, dentro de su clasificación como moneda virtual, prosiguiendo con un breve capítulo dedicado a la historia de su evolución y desarrollo.

A continuación, se presenta un capítulo dedicado a sus fundamentos más importantes a nivel tecnológico, y las tipologías más relevantes, que concluye con un comentario sobre las posibles aplicaciones de dichos fundamentos y en especial del Blockchain.

Seguidamente, se añade otro capítulo dedicado al mercado de las criptodivisas, en el que se explora en mayor profundidad las ventajas e inconvenientes que implica su uso en la práctica, así como recomendaciones y valoraciones sobre su utilización real por parte, sobre todo, de comerciantes y empresas, concluyendo con valoraciones acerca de los posibles escenarios futuros de las criptodivisas. Éste capítulo se ve sucedido por los resultados del estudio exploratorio a través de entrevistas breves realizadas a diferentes empresas que aceptan pagos mediante bitcoin (la criptomoneda más utilizada), que pretende alcanzar conclusiones sobre el modo de empleo actual e intereses de los negocios que optan por incorporarlo.

Por último, se exponen conclusiones relativas a las ventajas y desventajas que entrañan las criptodivisas en su aplicación real en la actividad comercial, comparándolas y concretando para el caso del bitcoin, que es la criptomoneda más utilizada.

Finalmente, en base a todo, se reflejan unas posibles líneas de mejora para el documento, de cara al futuro, así como un apartado de conclusiones y unos anejos recogiendo los formatos de entrevista y las respuestas.

2. CONCEPTO Y ORÍGENES DE LAS CRIPTOMONEDAS

2.1. CONCEPTO DE CRIPTOMONEDA

Uno de los países que se mantienen neutrales respecto del uso de las monedas virtuales en general y de aquellas conocidas como criptomonedas, en particular, es Estados Unidos y ya ha realizado esfuerzos para regularizar su existencia y uso, pudiendo acudir nosotros a las definiciones de moneda virtual que han establecido algunas de sus instituciones públicas:

> *"A diferencia de la moneda real, la moneda virtual es un medio de intercambio que opera como una moneda en algunos entornos, pero no tiene todos los atributos de una moneda real. En particular, una moneda virtual no es de curso legal en ninguna jurisdicción."*

(Financial Crimes Enforcement Network (FinCEN) 2013)

> *"Una moneda virtual es la representación digital de valor con el que se puede comerciar y funciona como un medio de cambio y/o unidad de cuenta y/o almacén de valor, pero no tiene curso legal en ninguna jurisdicción. No está emitida ni garantizada por ninguna jurisdicción y satisface las funciones señaladas sólo por el acuerdo dentro de una comunidad de usuarios de la moneda virtual. Es distinguida de la moneda fiat (también llamada moneda real, moneda nacional o dinero real), en que la última es la moneda y dinero papel de un país que es designado como de curso legal, circula y es habitualmente usado y aceptado como un medio de cambio en el país de expedición. Es distinta del e-money (dinero electrónico), que es la representación digital de la moneda fiat usada para transferir electrónicamente valor denominado en moneda fiat. E-money es un mecanismo digital de transferencia para moneda fiat, transfiere electrónicamente un valor de curso legal."*
>
> *"Moneda digital puede significar la representación digital de moneda virtual o e-money"*

(Financial Action Task Force (FATF) 2014)

A su vez, además de la diferencia que se explica respecto de la moneda convencional o fiat, en las mismas fuentes que las definiciones previas (FATF 2014; FinCEN 2013), se distingue moneda virtual convertible y no convertible, en función de si la moneda puede ser cambiada a moneda fiat y viceversa, o no; y también existe la clasificación en monedas virtuales centralizadas o descentralizadas, en función de si está involucrado un repositorio centralizado, cuyo administrador, debe permitir las transferencias de valor entre personas, o de si por el contrario, no hay administrador único o repositorio central y las personas pueden obtenerlas por sí mismas mediante capacidad de cómputo o esfuerzo de manufactura.

El término criptomoneda, se deriva de la criptografía, aquello que hizo posible la mayor parte de las monedas virtuales, tal y como se han definido, por ser algoritmos criptográficos sumados a protocolos de comunicación específicos, los que permiten asegurar la fiabilidad en los intercambios producidos en base a éstas monedas y según la FATF, la denominación criptodivisa, en concreto, se refiere a "monedas virtuales descentralizadas y basadas en las matemáticas, protegidas mediante la criptografía" (2014).

Así, aquí se estudiarán las monedas virtuales convertibles y descentralizadas (criptomonedas convertibles), si bien, existen ejemplos de monedas virtuales no convertibles, como las que se utilizan en el mundo de los videojuegos, por ejemplo el "oro" en el videojuego "World of Warcraft", o de monedas virtuales convertibles y

basadas en las matemáticas y la criptografía para su seguridad, pero centralizadas, como Webmoney, en poder de una empresa, que no satisfarían la definición de criptomoneda señalada.

2.2. HISTORIA Y ORIGEN DE LAS CRIPTOMONEDAS

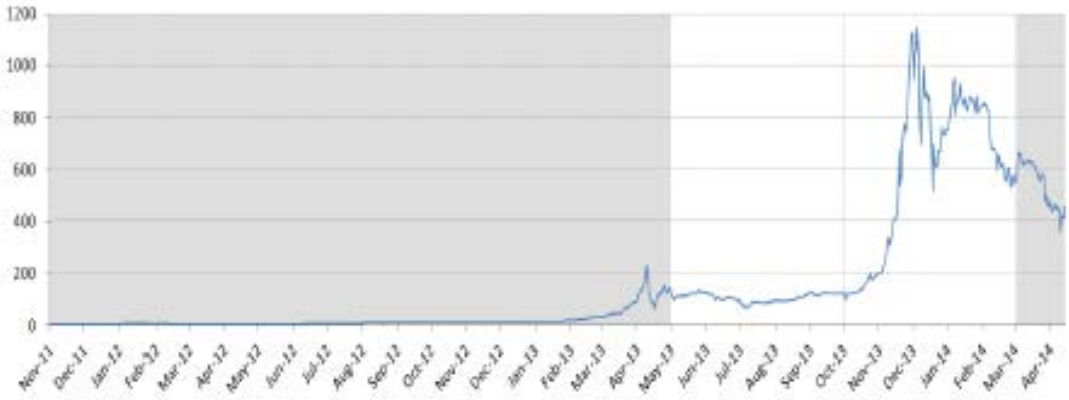
Durante la segunda mitad del siglo XX los avances realizados en cuanto a teoría de la información y criptografía, de la mano de expertos como Claud E. Shannon, Ralph C. Merkle, R.L. Rivest, … sentaron las bases para que se empezara a concebir la posibilidad, en la década de los 80, de aplicar la teoría sobre criptografía existente con el objeto de dar lugar a lo que hemos definido como criptomonedas. Uno de las más tempranos ejemplos es el caso de David Chaum, que en 1983, plantearía en artículos relacionados con el tema, como “Blind signatures for untraceable payments”, la posibilidad de utilizar sistemas de firma digital para realizar transacciones económicas privadas, verificables y susceptibles de ser bloqueadas en caso de fraude, y que dichas transacciones fueran supervisadas, en vez de por una entidad bancaria única, por un sistema descentralizado, como aquellos en los que se apoyan las criptomonedas actuales, por ejemplo, el Bitcoin (Chaum 1983).

Durante los años 90, surgieron algunas monedas virtuales, como DigiCash, en 1990, desarrollado por el propio David Chaum, o Webmoney (previamente mencionado), se desarrolló el comercio electrónico de mano de los bancos, sistemas de pago online, como Paypal, nacido en 1998 y distintas formas de dinero electrónico o e-money, acompañadas de curiosos ejemplos como el de E-Gold, una moneda virtual que permitía abrir cuentas con una cantidad de metales preciosos, o el de Liberty Reserve, de 2006, que permitía registrarse y transferir dinero sin apenas identificar a los titulares de las transacciones, empresas que fueron cerradas debido a que investigaciones policiales demostraron que constituían plataformas para distintos tipos de tráfico ilegal y blanqueo de capitales (FATF 2014; Dermot M. 2007).

Las criptomonedas propiamente dichas, no serían mencionadas como una aplicación real de la tecnología existente, salvo quizás las sugerencias sobre el B-Money de Wei Dai, hasta que en 2008, Satoshi Nakamoto, seudónimo del creador del Bitcoin (Craig Wright) cuya identidad ha sido desconocida hasta hace poco (mayo de 2016), publicó su artículo “Bitcoin: A Peer-to-Peer Electronic Cash System” en el dominio bitcoin.org, describiendo los fundamentos de la primera criptomoneda y la red que la sustenta. No fue hasta el 3 de Enero de 2009, cuando dicha red entró en funcionamiento, con la generación del primer bloque, manteniendo el BTC una capitalización de menos de un dólar hasta Febrero de 2011, con una máxima de 1151$/coin en 2013, después de una subida iniciada en mayo de ese año y especialmente acusada tras el cierre de Silkroad, un mercado negro cuyo capital en bitcoins, que ascendía a un equivalente de 3.200.000$, fue requisado en una operación contra los distintos tipos de tráfico ilegal que se realizaban a través de ella, por parte de las autoridades estadounidenses, en octubre de 2013, fecha que marca un antes y un después en su historia. A partir de entonces la cotización ha caído hasta la actual, mucho menor y más o menos estable (Yingjie 2015).

A partir del bitcoin, surgieron otros tipos de criptomonedas basadas en su mismo esquema de protocolo de seguridad red, “Proof of Work” (PoW), como Litecoin, en 2011, que pretendía mejorar la velocidad de procesamiento de transacciones (aspecto relevante y problemático de cara a su seguridad y escalabilidad), siendo momentos destacables los surgimientos de criptomonedas con base distinta, como Peercoin en 2011, pionero con el esquema “Proof of Stake” (PoS) u otras que utilizan el “Byzantine consensus” como Ripple.

Figura 2.1.: Etapas de la evolución del bitcoin, con referencia a los eventos acontecidos en 2013.



Fuente: Yginjie 2015.

3. FUNCIONAMIENTO Y FUNDAMENTOS CRIPTOGRÁFICOS BÁSICOS

3.1. FUNDAMENTOS TÉCNICOS Y CRIPTOGRÁFICOS BÁSICOS

Algunos conceptos técnicos relacionados con el tema son expuestos a continuación para poner de manifiesto cómo, a pesar de las críticas, la solidez de los fundamentos tras las criptodivisas está fuera de toda duda. Se hace referencia especialmente al caso del bitcoin, por su mayor repercusión.

3.1.1. Firma digital

En primer lugar, los algoritmos de criptografía de clave pública, que también se han utilizado, como en el caso de RSA (Rivest, Shamir y Adleman) en el protocolo SSL (Secure Socket Layer) conjuntamente con criptografía simétrica, para asegurar las transacciones económicas tradicionales en internet y establecer sesiones seguras en entornos que no suelen serlo a priori; juegan un papel fundamental en la identificación de las partes de una transacción realizada mediante una criptodivisa.

En el caso del bitcoin, el algoritmo utilizado es el ECDSA (Elliptic Curve Digital Signature Algorithm), basado en la criptografía de curvas elípticas (ECC), en su versión de fortaleza 128bits y tamaño de clave 256bits, que correspondería en el algoritmo RSA anteriormente citado y basado en la factorización de grandes números compuestos, a un tamaño de clave de 3072bits, resultando, por tanto, más eficiente el primer método.

En cuanto a su funcionamiento, ECC está relacionado con un problema matemático llamado ECDLP (Elliptic Curve Discrete Logarithm Problem). Así, estos criptosistemas inventados por Neal Koblitz y Victor Miller en 1985 se basan, además de en la geometría de dichas curvas, en el concepto de los logaritmos discretos, que operan en el dominio de los números enteros e involucran conceptos de teoría de grupos que no vamos a desarrollar aquí, aunque también tienen gran importancia en otros sistemas como DSA (Digital Signing Algorithm), DH (Diffie-Hellman) o El Gamal.

3.1.2. Hash

Unas funciones muy utilizadas en los protocolos de las criptomonedas son las funciones hash. Como se explica en la lección de “Introducción a bitcoin” de Cript4you (2014), toman una entrada datos de cualquier longitud y devuelven una cadena de bits de longitud fija (hash), siendo sus características deseadas para la aplicación en criptografía:

- **Eficiencia en la computación**. Cálculo rápido.
- **Resistencia a preimagen**. Debe ser muy difícil recrear el mensaje a partir del cual se ha derivado el hash.
- **Resistencia a segunda preimagen**. Debe ser muy difícil, dado un mensaje, obtener un segundo con el mismo hash.
- **Resistencia a colisión**. Debe ser muy difícil crear dos mensajes distintos con el mismo hash.

Además, las funciones hash tienen la propiedad de ser “Puzzle friendly”. El Puzzle sería encontrar un valor, que procesado por una función (hash) junto con otro valor

aleatorio, haga que la salida caiga dentro de un conjunto objetivo. Así, esta propiedad garantizaría que la única posibilidad de resolver tal problema sería probar con todas las posibles soluciones, lo que fundamenta las expresiones de validación de bloques en los protocolos de las criptomonedas (Narayanan et al. 2016).

Los hashes han tenido diversas aplicaciones en firmas digitales, algoritmos de autenticación, fingerprinting o también para verificar la integridad de datos, como veremos más adelante. En bitcoin se utilizan los siguientes dos tipos:

- **SHA-256** (Secure Hash Algorithm). El principal, de la família SHA-2 diseñadas por la NSA y aceptadas como estándar del NIST para sustituir SHA-1.
- **RIPEMD-160** (RACE Integrity Primitives Evaluation Message Digest). Bitcoin lo usa para hashes de menor longitud. Nacido en 1996, pertenece a la familia RIPEMD, de longitudes de salida de 128, 160, 256 y 320 bits. Bitcoin usa la versión de 160 bits, como SHA-1, pero fue creado por una comunidad abierta.

SHA-256, en concreto, se haya compuesto de tres mecanismos diferenciados que son los que siguen y se representan en la figura 3.1. (Boneh 2015):

- Un cifrado de bloque: En éste caso SHACAL-2, algoritmo de cifrado de 512bits de clave y 256bits de mensaje y salida (otros ejemplos serían AES, …).
- Una función de compresión: en el caso de SHA-256 es la de Davies-Meyer, (también existen diversos ejemplos de estas funciones como Whirlpool, …).
- La transformada de Merkle-Damgard: consiste en la ejecución en serie de hashes para posibilitar una entrada de cualquier tamaño a la función hash.

Cabe destacar que los hashes en Bitcoin son resultado de aplicar dos veces un algoritmo de hash sobre cualquier dato, para incrementar la seguridad.

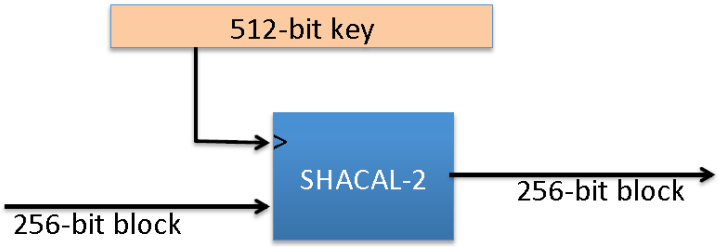
3.1.3. Merkle trees e integridad entre nodos

Se trata de la agrupación por parejas de bloques de datos (hojas del árbol) a cada uno de los cuales se aplica un hash que se sigue ejecutando sobre las parejas de resultados hasta conseguir un único valor, denominado Merkle root. Éste se utiliza a modo de comprobación de la integridad del conjunto de los datos, que pueden incluirse en el mismo mensaje, al deber reproducirse el proceso con el mismo resultado, a menos que un atacante haya modificado el contenido en el camino.

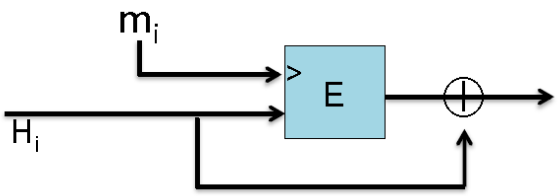
Además, se podría realizar una comprobación de pertenencia de cada bloque de datos al Merkle Tree, a través del camino definido por las correspondientes ramas hasta la raíz, verificando un número de hashes mucho menor que el total (n), en concreto serían necesarios sólo log(n).

Está relacionado con el concepto de las cadenas de hash donde el coste de verificación de un elemento es proporcional linealmente al número de hashes (y no al logaritmo del mismo) (Narayanan et al. 2016).

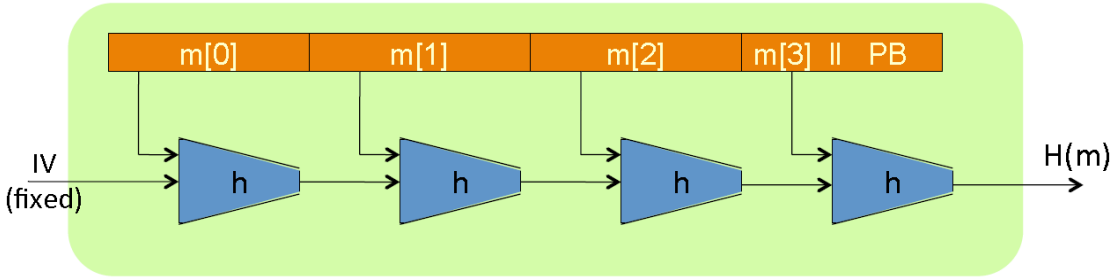
Figura 3.1.: Componentes de SHA-256



Shacal-2



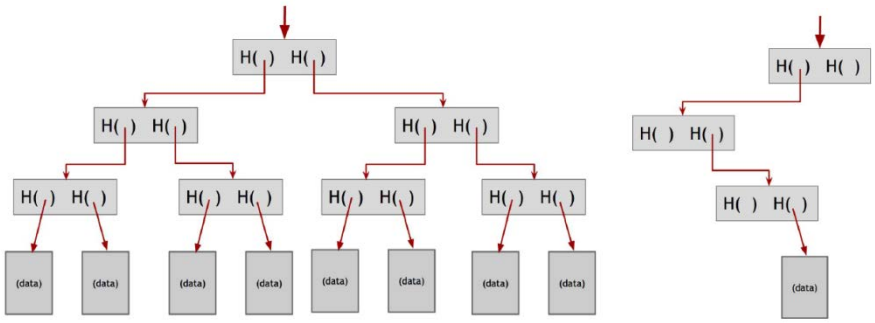
Función de compresión Davies-Meyer



Paradigma de Merkle-Damgard

Fuente: Boneh, D. 2015.

Figura 3.2.: Merkle Tree



Fuente: Narayanan et al. 2016

3.1.4. Blockchain como base de datos distribuida

La realidad de funcionamiento de cualquier criptomoneda se refleja en el estado del blockchain, que es una colección de salidas de transacción no gastadas (UTXO), bloqueadas criptográficamente. Así, se guardan las transacciones realizadas desde los bloques de origen.

Si consideramos la red como una base de datos distribuida, en téminos de CAP (Consistency, Availability y Partition-tolerance), cumple en cuanto a disponibilidad (toda petición recibe respuesta), y tolerancia a la partición (el sistema sigue funcionando si algunos nodos fallan) pero no es consistente siempre, puesto que, aunque pueden estar descubiertos los hashes de los nuevos bloques, no tienen por qué conocerse por todos los usuarios, en todo momento. Sin embargo, como se menciona en el artículo de BitFury Group de 2015, que desarrolla las diferencias y características entre PoS y PoW y en el que nos hemos basado para elaborar buena parte de éste apartado, para conseguir una consistencia eventual se requiere:

- Los bloques descubiertos deberían ser inmediatamente emitidos en la red sin estar incentivada la retención de los mismos por los nodos.

- Los nodos deben ser disuadidos de minar sobre bloques intermedios de las cadenas.

- Las reglas de consenso deberían plantearse de modo que, en los forks, las ramas correctas sobrepasasen con una rapidez suficiente a las demás en competencia.

Con éste fin existen los esquemas de prueba de dificultad en la validación de los bloques, como PoW y PoS o las condiciones inherentes al RPCA, relacionadas en primera instancia con la confianza cuya necesidad en el proceso tratan de eliminar la mayoría de las criptomonedas. A continuación, señalamos cómo funcionan algunas criptodivisas en base a estos esquemas de protocolo.

3.2. PROOF OF WORK (BITCOIN)

Aquí se expone de modo sencillo cómo opera la red de Bitcoin para hacer posible su función de criptodivisa, en base al artículo original de Satoshi Nakamoto de 2008 y al artículo de BitFury de 2015 que ya se ha mencionado anteriormente.

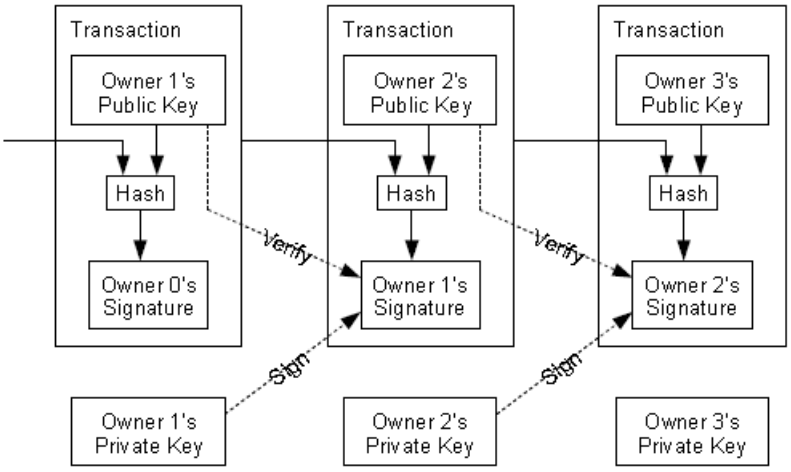
Cada transacción en la red de bitcoin representa una cantidad de la criptodivisa y es el hash de la transacción previa por la que se ha adquirido y la clave pública del destinatario de la siguiente, firmado por el emisor de la misma con su clave privada. Así, se pretende garantizar la correcta identidad de las partes y el receptor del pago puede utilizar las firmas para verificar la cadena de propietarios, como sucede con todos los sistemas de criptodivisas.

Las transacciones permiten múltiples inputs y outputs con el fin de que los bitcoin sean divisibles.

Queda garantizar la no presencia de dobles gastos de la misma cantidad de criptodivisa, relacionada como hemos visto, con la consistencia del blockchain como base de datos. En una moneda tradicional, se soluciona a través de una entidad intermedia, central, que almacena el historial de pagos completo y decide cuáles son válidos. Para las criptodivisas, se resuelve publicando el historial de transacciones en una red, en la que los participantes acuerdan qué orden es el válido y lo almacenan. Para esto, se graba una marca temporal o timestamp en los bloques, que son entrada

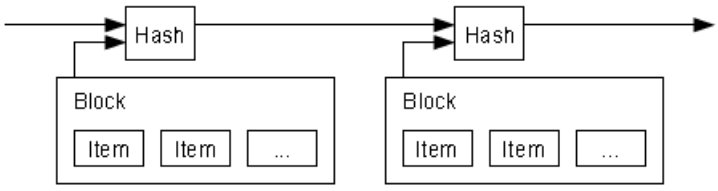
de un hash, sirviendo el resultado, a su vez, de entrada del hash del siguiente bloque con su timestamp.

Figura 3.3.: Proceso de firma de transacciones.



Fuente: Satoshi Nakamoto 2008

Figura 3.4.: Cadena de bloques (cadena de hash).



Fuente: Satoshi Nakamoto 2008

Así, se mantiene un servidor de timestamp distribuido, conjuntamente con la base de datos distribuida que constituye el blockchain, cuya consistencia (y el doble gasto) se ve mantenida en bitcoin por un sistema PoW similar al Hashcash de Adam Back, buscándose mediante el incremento de un nonce incluido en cada bloque, un valor que al alimentar un hash (SHA-256), produzca un determinado número de 0 en la salida, para satisfacer el esfuerzo de cómputo requerido por la red. La cadena de bloques (cadena de hash) hace que el coste para un atacante de producir forks fraudulentos sea proporcional linealmente al número de bloques a partir del objetivo del doble gasto.

El concepto de prueba de trabajo (PoW) es el más antiguo y utilizado en el bitcoin, fue ideado en 1993 por Cynthia Dwork y Moni Naor como un conjunto de datos, costosos de producir satisfaciendo ciertos requisitos, pero sencillo de verificar.

Si entramos en profundidad en la validación de los bloques, podríamos empezar comentando que cada uno consta de un encabezado con parámetros fundamentales como el momento de creación del bloque, referencia al bloque anterior, versión, objetivo actual, nonce y raíz del árbol de merkle de las transacciones, y un cuerpo formado por la lista de transacciones. Para realizar el PoW, una vez definido el nonce del encabezamiento, se realiza un hash dos veces, con SHA-256 (nosotros

utilizaremos la expresión “hash()”), resultando un entero en el intervalo $[0, 2^{256} - 1]$ ([0, M]). Para que un bloque sea válido debe satisfacer:

$$\text{hash}(B) \leqslant M/D$$

Donde $D \in [1; M]$ es la dificultad objetivo. Por una propiedad de los hashes comentada, no hay modo conocido de conseguir satisfacer la expresión sin probar una por una todas las posibilidades, con lo que cuanto más alto sea D, más trabajo y energía requerirá hacerlo. Por otras propiedades de las funciones hash, la expresión anterior es un caso particular de:

$$U \leqslant \theta \leqslant 1$$

Donde U es una variable aleatoria de distribución uniforme producida mediante el hash de ciertos datos, siendo $\theta = 1/D$. Para generar el bloque U debe satisfacer la condición señalada. N son las combinaciones que un usuario necesita evaluar antes de encontrar un bloque válido. El espacio de búsqueda es amplio para PoW, pudiendo iterar en r combinaciones por segundo, donde r está determinado por el hardware disponible y puede tomar un valor infinito en teoría. Si T es el tiempo que toma a un usuario encontrar un bloque válido $T = N/r$, se puede considerar la siguiente distribución de probabilidad acumulada:

$$P(T \leqslant t) = P(N \leqslant rt) = 1 - P(N > rt) = 1 - (1 - \theta)^{rt} = 1 - \exp(\log(1 - \theta)^{rt})$$

Si $\theta \ll 1$, como suele ocurrir:

$$\log(1 - \theta) \approx -\theta;\ P(T \leqslant t) \approx 1 - \exp(-\theta rt)$$

Luego T está distribuido exponencialmente con tasa θr que es r/D para el caso de PoW.

Debido a las propiedades de las distribuciones exponenciales, la expresión queda de la siguiente manera si consideramos n mineros con tasas de hash de $r_1, r_2, \ldots, r_i$ siendo T el mínimo valor de entre las variables aleatorias T(r_i), asumiendo que los bloques alcanzan a los otros nodos inmediatamente cuando son publicados:

$$P\left(T_{def} = \min(T_1, \ldots, T_n) \leqslant t\right) = 1 - \exp\left(-\frac{\mathrm{t}}{\mathrm{D}}\sum_{\mathrm{i}=1}^{\mathrm{n}} r_i\right)$$

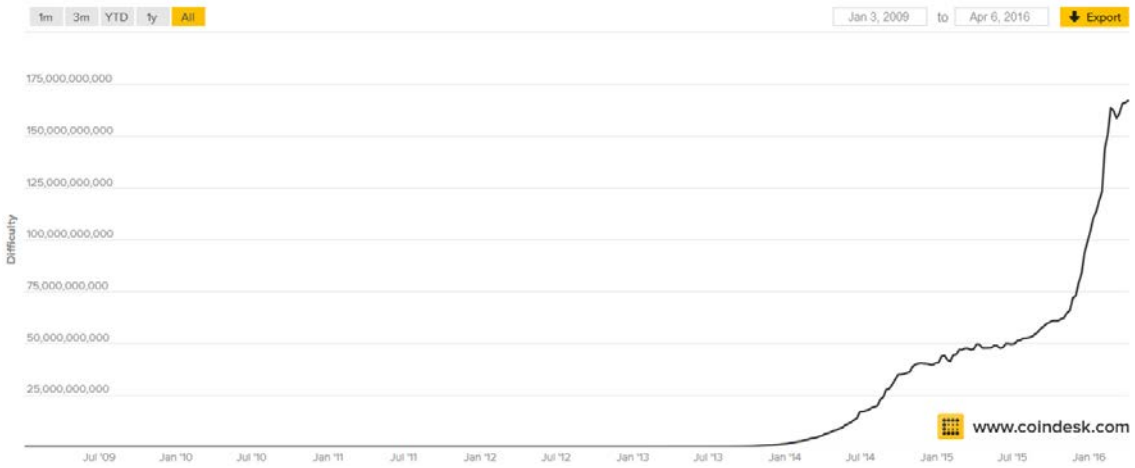
$$P(T = T_i) = 1 - \exp\left(-\frac{r_i}{\sum_{\mathrm{j}=1}^{\mathrm{n}} r_j}\right)$$

Esto demuestra que la minería es justa para nodos de igual capacidad de computación, al tener igual probabilidad de resolver un bloque.

Éste sistema resuelve lo que sería un sistema de decisión basado en la votación de la mayoría, fundamentado en el principio una CPU un voto, en vez de una IP un voto. Así, si la mayoría de los nodos son de confianza, la cadena de bloques generada a partir del ganador de la prueba de trabajo, crecerá rápidamente frente al resto y corresponderá a la más larga.

Para compensar la incremental velocidad del hardware, la dificultad es determinada por la media, variable, cada 2016 bloques, con el objetivo de procesar un número determinado de bloques por hora. Es decir, si los bloques son generados demasiado rápido, la dificultad se incrementa, buscándose unos 6 bloques por hora.

Figura 3.5.: Evolución de la dificultad en la historia del bitcoin.



Fuente: www.coindesk.com (6 Abril 2016)

En cuanto a la red, funciona de la siguiente manera:

1. Las nuevas transacciones son enviadas a nodos.
2. Cada nodo aúna las transacciones en bloques.
3. Cada nodo realiza su PoW sobre cada bloque producido.
4. Cuando encuentra su PoW el nodo envía su bloque a los demás.
5. Los nodos verifican la validez y doble gasto de las transacciones del bloque.
6. Los nodos expresan su aceptación del bloque, usándolo como base para la creación del siguiente, a través del hash del primero.

Cuando un nodo recibe más de un bloque válido simultáneamente, o se producen varias cadenas distintas, en distintas partes de la red, el nodo guarda todas las opciones y considera válida la rama que se convierte en la más larga.

Las transacciones no alcanzan todos los nodos, pueden ser procesadas en una región de los mismos e ir añadiéndose a bloques, con el tiempo. Los bloques también pueden perderse y los nodos los requerirán cuando reciban el siguiente a los mismos, percatándose de dicha pérdida.

La primera transacción de un bloque es especial (coinbase) y comienza una nueva cadena, en la que el creador del bloque es propietario de los nuevos bitcoin asociados, lo que se hará realidad si logra ejecutar el PoW antes que el resto de los nodos. Éste es el incentivo de los mineros o propietarios de los nodos, además de la existencia de transaction fees, consideradas cuando la salida de una transacción es menor que su entrada, siendo la diferencia, la tasa de recompensa para los nodos que las verifiquen. Una vez que el número total de bitcoins, fijado en 21 millones, sea alcanzado, se verá libre de inflación y éste tipo de tasas serán el único incentivo de los nodos.

Como se comentan Narayanan et al. (2016), las transaction fees sólo se aplican cuando las transacciones cumplen lo siguiente:

- Son menores de 1000 bytes
- Todas las salidas son de 0,01 BTC o mayores
- La prioridad es suficientemente grande:

$$Prioridad = \frac{suma\ de\ edades\ de\ las\ entradas\ x\ valor\ de\ la\ entrada}{tamaño\ de\ la\ transacción}$$

Si no se cumple alguna de las condiciones, se aplicaría una tasa de alrededor de 0,0001BTC por cada 1000bytes de transacción. Hay que tener en cuenta que cada transacción implica como mínimo 148bytes por entrada, 34bytes por salida y 10bytes por otra información necesaria.

En cuanto a los posibles ataques, que son valorados más en profundidad en otro apartado, Satoshi Nakamoto arguye que el incentivo de poder crear más nuevos bloques por parte de un nodo desleal que posea la mayoría del poder de cómputo de la red, lo empujará a evitar destruirla por su capacidad de adquirir más riqueza.

Además, si la red no está controlada por nodos fiables podría existir riesgo de albergar transacciones falseadas, estableciéndose un sistema de alertas de la red, para casos de transacciones inválidas, incitando al cliente a la descarga de los bloques y alertas, siendo interesante, además, especialmente para negocios, el establecer sus propios servidores, por agilidad en la verificación y mayor seguridad.

En cuanto al anonimato en las transacciones, se pierde al ser hechas públicas, a menos que se oculte deliberadamente quién está detrás de cada clave pública. Se puede reforzar también originando nuevos pares de claves en cada nueva transacción. Para transacciones con múltiples entradas, se da la circunstancia de que, si es dilucidada la identidad de una de las claves, se desvelaría la del resto de las mismas. Este posible anonimato de las transacciones es el que ha incentivado a defraudadores y criminales a utilizar ésta criptomoneda como medio de conquistar el mercado virtual, aunque su carácter público también está ayudando a las autoridades a encontrar a muchos.

3.3. PROOF OF STAKE (PEERCOIN) Y SUS POSIBILIDADES COMO EXTENSIÓN DE PROOF OF WORK

Pretendiendo subsanar el problema a largo plazo del consumo de energía para mantener la seguridad y el de aumento de la latencia con el tiempo, Sunny King y Scott Nadal, propusieron en 2012, PPcoin (Peercoin), el primer sistema de criptodivisa incorporando PoS. Descubrieron que la prueba de tenencia es difícilmente reproducible, y utilizaron el concepto de “coinage”, para evitar el doble gasto, que se utilizaba en el PoW del bitcoin pero sin jugar el mismo papel. Éste consiste en la cantidad de coins poseídos multiplicada por el tiempo durante el cual se poseen. Aquí desarrollamos los fundamentos básicos del PoS partiendo del artículo original de dichos autores y de nuevo, el artículo de BitFury de 2015.

Peercoin es un híbrido en el que existen bloques de PoW y de PoS. La prueba de tenencia en el segundo caso, utiliza una transacción especial llamada coinstake, similar al coinbase, en el que el minero se paga a sí mismo, consumiendo su coinage. El primer parámetro del coinstake se llama kernel y debe cumplir ciertos requisitos al ejecutarse un hash sobre él, siguiéndose una casuística similar a la de PoW, sólo que el hash es ejecutado sobre un espacio de búsqueda limitado, un hash por UTXO, por segundo (coinage), a diferencia de PoW (ilimitado), limitando el consumo energético y la velocidad de procesado. En éste caso, además, los objetivos de hash de PoW y PoS son reajustados continuamente, en vez de cada dos semanas, como con bitcoin.

Si se aborda algo más en profundidad la validación de los bloques en la red, empezando por el PoS puro (distinto de Peercoin), se mantendría la validez de la expresión $U \leqslant \theta \leqslant 1$ del caso de PoW, si bien, la tasa de la distribución exponencial

tendría como valor bal(A)/D, siendo A la dirección de un usuario y bal(A) su balance, lo que convierte el esquema en justo, dependiente de la cantidad de moneda poseída por el propietario del nodo respecto de la cantidad total en la red. Entrando en profundidad, la expresión que se ha de satisfacer para validar un bloque sería la que sigue:

$$\text{hash}(\text{hash}(B_{prev}), A, t) \leqslant \frac{\text{bal}(A)M}{D}$$

Encontrándose el balance criptográficamente bloqueado por el protocolo, es t, el timestamp, la única variable susceptible de ser modificada, que sin embargo deberá cumplir ciertas restricciones respecto de la hora de la red. El espacio de búsqueda es pequeño y se puede considerar frente al PoW un número de combinaciones por segundo de r=1, al buscarse que no influya la capacidad de cómputo en el proceso.

El tiempo para encontrar un bloque de la red completa está distribuido exponencialmente con una tasa $\sum_{\text{a}} \frac{bal(A)}{D}$, luego si el suministro monetario es fijo o crece a una tasa predecible, la dificultad D será la que sigue, siendo T_{ex}, el tiempo esperado entre bloques:

$$D = \frac{1}{T_{ex}} \sum_{\text{a}} bal(A)$$

En el caso particular del Peercoin, la parte de PoW es similar al bitcoin, pero se basa en el coinage para la parte PoS, siendo la condición de validación, si consideramos U, la cantidad no gastada de Peercoin:

$$\text{hash}(\text{hash}(B_{prev}), U, t) \leqslant \frac{\text{bal}(U)\text{age}(U)M}{D}$$

age(U) es el tiempo tras la generación de U e influye en la probabilidad de encontrar un bloque, conjuntamente con la cantidad de coins acumulada, que se mencionaba en el caso del PoS puro.

Pese a que en PPcoin se mantiene PoW para mejorar el proceso de minado inicial, en el caso de un sistema PoS puro, se debería comenzar en un bloque de origen único, que produciría problemas como los de posible fraude que se comentan más adelante.

En cuanto al consenso, como hemos explicado, se alcanza validando la cadena con más coinage consumido. Además, pese a necesitarse el control del poder de minado del 51% de la red para un ataque, igual que con PoW, los creadores del PPcoin argumentan que es más complicado acumular una cantidad significativa de coins que de poder de computación y el coinage consumido una vez, previniendo ataques sucesivos, aunque hay autores que sostienen lo contrario en sus trabajos, como Nicolas Houy (2014). Si bien, aunque esto fuera cierto, la seguridad del blockchain es más difícil de mantener frente al PoW del bitcoin, y el protocolo ha sido constantemente revisado para subsanar distintos fallos. Además, puede ser necesaria menor cantidad de coinage para obligar al blockchain a reestructurarse, así que es imperativo utilizar puntos de comprobación que deberían difundirse desde servidores centralizados, similares a los checkpoints del sistema de alertas de bitcoin, dado que no ha sido diseñado aún un sistema parecido que funcione de forma distribuida. En el bitcoin éstos tienen una fecha de caducidad para adaptarse al modelo, pudiendo verificar la conexión de los coinbase antes de añadirse los nuevos bloques al blockchain. Los creadores del PPcoin, propusieron dotar al coinage de un mínimo, correspondiente a un tiempo de posesión de un mes, sirviendo los checkpoint para transacciones de más de un mes.

Por otro lado, para el escalado de la dificultad se utilizan funciones continuas, frente a las escalonadas de bitcoin, para evitar el impacto del cambio en el mercado.

Las transaction fees son eliminadas por ser vistas como incentivo de no cooperación entre mineros y de rechazo del reconocimiento de bloques de otros mineros, para contrarrestar la fuerza inflacionaria de la minería y para evitar posibles ataques de inflado de bloques (block bloating attack) que, entre otras cosas, aumenten el tamaño del blockchain desproporcionadamente.

3.4 BIZANTINE AGREEMENT (RIPPLE)

Como ejemplo un tanto alejado del concepto de criptomoneda, por su carácter más centralizado en torno a los intereses del sector financiero actual y creada a partir de un sistema o protocolo ligeramente distinto a los anteriores, Ripple es un caso de intento de aplicación de las criptotecnologías detrás del bitcoin y los esquemas anteriores para satisfacer los intereses de las citadas entidades financieras, con una filosofía distinta e ideado por una startup del mismo nombre. Aquí se especifica cómo el fundamento de dicho sistema es la raíz de los anteriores, el blockchain, aunque aplicado como si fuera un mero método de pago o transferencia electrónica de activos. Para ello, se ha recurrido al artículo de David Schwartz, Noah Youngs y Arthur Britto, titulado “The Ripple Protocol Consensus Algorithm”, de 2014.

Los sistemas de pago distribuidos presentan tres problemas fundamentales: distinguir transacciones correctas e incorrectas (corrección), acuerdo para evitar fraudes mediante transacciones correctas, como el de doble gasto (acuerdo), y utilidad, por el tiempo en que se ejecutan, recursos que necesita el sistema, … Esto, según los autores de Ripple, ya fue abordado en tiempos antiguos a través del “Problema de los Generales Bizantinos”, en el que un ejército, dividido en unidades controladas por lugartenientes, recibe órdenes del comandante general de avanzar o retroceder, pero como no todos los generales son leales y los mensajes se pueden perder en el camino o ser interceptados por el enemigo, los lugartenientes deben consensuar en qué orden obedecer, enviándose mensajes firmados entre sí. Los individuos en estos sistemas se unen a servidores que se comunican entre sí y deben decidir si los mensajes (transacciones) que reciben de los otros, son verdaderos (su misión es comunicarse y alcanzar un consenso). En Ripple, cada servidor tiene una Unique Node List (UNL), con los nodos “de confianza” con los que sólo se puede comunicar y votar transacciones para buscar el consenso, aunque no necesariamente se deben considerar a todos éstos nodos como de confianza. Hay un “Ledger”, similar al Blockchain, que es un libro mayor compartido de las transacciones aceptadas por consenso, un “Last-Closed Ledger”, que representa al último Ledger aceptado por consenso, y un “Open Ledger”, que es el actual estado de operación de un nodo, cuyas transacciones aún no han pasado por consenso y por tanto no puede convertirse en un “Last-Closed Ledger”. Por último, tenemos el concepto de “proposer” correspondiente a todos los servidores, dado que todos pueden incluir transacciones en el proceso de consenso cada nueva ronda, aunque sólo participarán en el mismo, aquellos en la UNL.

Los nodos pueden fallar (por errores no intencionales o los que sí lo son, conocidos como Bizantinos). Se define consenso de acuerdo a 3 axiomas:

- Todo nodo correcto toma decisiones en tiempo finito.
- Todo nodo correcto alcanza el mismo valor de decisión.
- 0 y 1 son respuestas posibles para cualquier nodo correcto (evitando los que siempre responden uno de los dos valores).

La posibilidad de intercambiar mensajes de modo asíncrono (sin límites de tiempo de decisión) daría pie al no cierre del algoritmo incluso con un sólo proceso incorrecto, necesitándose heurística basada en el tiempo para garantizar la convergencia. La fortaleza de un algoritmo de consenso se suele medir por los procesos erróneos que tolera y es probable que ninguna solución del "Problema de los Generales Bizantinos" que asuma un carácter síncrono, con agentes conocidos, tolere más de un tercio de la red de errores Bizantinos, permitiendo, aun así, mayor porcentaje de errores que el caso asíncrono, pese a no requerirse autenticidad de los mensajes entre nodos (firma de transacciones). Sin embargo, hay muchas alternativas de algoritmos asíncronos que toleran hasta el 20% de errores Bizantinos, como el FaB Paxos, o incluso los hay que resuelven el caso asíncrono con participantes desconocidos, para un tercio de errores Bizantinos, pero con restricciones sobre la red adicionales, como el BFT-CUP.

En éste caso, es el RPCA (Ripple Protocol Consensus Algorithm), el encargado de resolver la corrección y acuerdo, cada pocos segundos. Se cierra el Open Ledger cada vez que se alcanza el consenso, compartiéndose ésta información entre los nodos en caso de no existir forks por la pertenencia de los aquellos a distintas UNL. Funciona así:

- Cada servidor emite una "lista de candidatas" con todas las transacciones sobre las que no se ha resuelto el consenso.
- Los servidores recogen las candidatas recibidas de su UNL y las vota.
- Las rechazadas serán eliminadas o incluidas en el proceso siguiente de consenso.
- La última ronda requiere una aceptación del 80% de la UNL, para ser incluidas en el Last-Closed Ledger.

Dado que se requiere la aceptación de las transacciones por el 80% de los nodos, aunque falle la corrección, si el número de nodos fallidos es mayor al 20%, sería necesario más de (4n+1)/5 errores Bizantinos, para que una transacción incorrecta fuese confirmada. El primer umbral será el de corrección fuerte y el segundo el de corrección débil.

La siguiente expresión define la probabilidad de que el número de errores permanezca por debajo de los aceptables (de corrección):

$$\sum_{i=0}^{\left\lceil\frac{(n-1)}{5}\right\rceil} \binom{n}{i} p_c^i (1-p_c)^{n-i}$$

p_c Indica la probabilidad de que un nodo se convierta en desleal. Así, dado que la distribución de la probabilidad es binomial, podemos elegir el UNL tratando de minimizar p_c, que habrá de ser como máximo del 20%. Como los nodos, países… son criptográficamente identificables, seleccionar UNL de naciones, intereses, … dispares facilitará un p_c por debajo del 20%. Incluso si el UNL tiene un p_c relativamente grande, de digamos, un 15%, la probabilidad de corrección es alta, aunque sólo haya 200 nodos en el UNL (97,8%).

En cuanto a la posibilidad de forks, se establece un solapamiento mínimo del 20% del total de nodos componentes de la UNLs compartidas en dos o más grupos separados, como límite para que se puedan invalidar transacciones ya verificadas por consenso.

Por otro lado, como hemos dicho, es necesario una limitación de la latencia del proceso para garantizar la convergencia de la decisión sobre la corrección, pero hay otras heurísticas y límites que proporcionan utilidad al RPCA:

- Hay una ventana de 2 segundos para que los nodos emitan sus conjuntos de transacciones sugeridas. Esto introduce un límite inferior de la ronda de consenso y garantiza que sólo intervengan los nodos con latencia razonable.

- Según los nodos son grabados en el "ledger" para cada nueva ronda de consenso, pueden ser marcados y eliminados de la red por malos comportamientos identificables, como los que no votan todas las transacciones y los que proponen constantemente transacciones no validadas.

- Un algoritmo de detección de divisiones en la red es empleado para evitar forks, dado que el algoritmo de consenso no impide que varios Last-Closed Ledger coexistan, por dificultades en la comunicación entre ellos. Para evitarlo, cada nodo escanea el tamaño de sus miembros activos en la UNL, identificándose la división de la red cuando el tamaño cae por debajo de cierto umbral. Para evitar falsos positivos, si hay una región de la red que tiene cierta latencia, los nodos pueden publicar una "validación parcial", en la que declaran que aún están participando en el proceso de consenso y no están participando en otro, ni están desconectados de la red.

- Aunque podría aplicarse una sola ronda en el RPCA, se puede ganar utilidad introduciendo más, cada una con más porcentaje de acuerdo necesario. Estas rondas permiten la detección de nodos latentes en el caso de que produzcan cuellos de botella en las tasas de transacciones, que son identificados cuando el porcentaje de tolerancia de fallos alcanza cierto valor. En una sola ronda, podría ser que tan pocas transacciones superaran el umbral del 80%, que se ralentizara la red entera más allá de la latencia de los nodos más lentos.

3.5. OTRAS APLICACIONES DETRÁS DE LOS FUNDAMENTOS TECNOLÓGICOS DE LAS CRIPTODIVISAS (BLOCKCHAIN)

Utilizando como referente el informe del grupo de trabajo en pagos electrónicos y alternativos de la EBA, de 2015, de título "Cryptotechnologies, a major IT innovation and catalyst for change", se puede contemplar una clasificación de las criptodivisas en el mercado, en función de las utilidades fundamentales que dan al blockchain:

- Criptomonedas: casos como el Bitcoin, Litecoin, Peercoin o Dogecoin. Ésta es la perspectiva que hemos asumido como eje del trabajo.

- Registro de activos ("asset registry"): utilizan libros de contabilidad públicos para registrar activos distintos de los propios coin, incluyendo transacciones referidas a acciones, vehículos,… El propietario de los mismos es registrado en la red sin supervisión de una autoridad central, contando con la clave privada de dicha transacción. Los registros públicos tienen potestad de cierto gobierno y auditoría de costes. Algunos ejemplos son Mastercoin o Counterparty. Sin embargo, ésta tecnología conlleva la inclusión de datos adicionales al blockchain que implican la no escalabilidad del sistema. Factom, por ejemplo, es una tecnología en desarrollo que está solucionando esto deshaciéndose de los citados datos antes de incorporarlos al blockchain.

- Pila de aplicación ("application stack"): NXT o Ethereum, por ejemplo, buscan aplicar la tecnología blockchain para el desarrollo y ejecución de aplicaciones escalables sobre redes descentralizadas, que se podrían comparar a una

especie de servicio en la nube y podría generar oportunidades en cuanto a pagos, por la posibilidad de creación de ofertas con un grado de personalización elevado. El caso está relacionado con el concepto de aplicaciones distribuidas o Dapps.

- Centrados en activos ("asset centric"): basados en el intercambio de la representación digital de activos, en base a un libro contable compartido, pero no público (caso de Ripple o Hyperledger). La confianza está fundada directamente en los participantes (PSPs, Bancos Centrales, …) y no en los mineros y el blockchain. Los participantes de la red publican activos digitales en ella como dólares, bitcoins, … y algunos de éstos participantes son responsables de convertirlos del mundo físico al digital (gateways). Para el intercambio se requiere al conocido como "market maker", una institución extranjera de cambio de gran volumen. Se pueden crear acuerdos de cambio exclusivos y permitiría reducir costes en entidades bancarias y mejorar productos y velocidades de procesamiento, con las siguientes aplicaciones:

    - Transacciones forex: el ofrecimiento de servicios entre países diferentes, implica operaciones entre cierto número de entidades que conlleva un elevado coste por su complejidad. Si se ofrece forex en consenso distribuido, los PSPs de distintas jurisdicciones actuarán como gateways publicando sus activos digitales y una vez establecen mutua confianza, pueden comerciar. Pueden usar también los "market makers" para proveer de liquidez al mercado cuando sea necesario, y como puente, para realizar transacciones posteriormente y no contarían con los altos costes citados.

    - Pagos instantáneos: permite a los bancos de diferentes jurisdicciones operar en transferencias con una casuística similar a la antes mencionada con los PSPs, siendo habitual el ejemplo aquel en el que se utiliza un banco central como "market maker" proveedor de liquidez.

    - Gestión documental: aunque los PSPs han recurrido a los medios digitales para la gestión de su patrimonio desde sus inicios, sus documentos se mantienen, en gran medida, en formato papel. Las wallet multifirma y la transparencia extrema a extremo de las transacciones, favorecen como opción a las criptotecnologías, además de la posibilidad de automatización de procesos.

    - Servicio de activos: si consideramos la aplicación de las criptotecnologías en éste aspecto, se referiría a la creación de activos (monedas, bonos, acciones, …), la facilitación del comercio entre bancos y otras instituciones y la posible liquidación de la posición de un inversor. El servicio de activos estaría encima de una serie de capas sobre el libro contable distribuido correspondiente al blockchain, capas necesarias para la legalidad del proceso, complejo, que precisa de la coordinación de los siguientes stakeholders: custodio de fianzas (autorizado para la creación de ciertos activos), custodio de moneda (que garantiza la correspondencia del activo con una cantidad en moneda fiat y podría ser un banco conectado al libro mayor distribuido), creadores (pequeñas entidades financieras intermediarias que venden estos activos a los clientes) e inversores (los clientes que adquieren dichos activos para percibir un beneficio a largo o corto plazo).

Desde 2014, Fidor Bank de Alemania ha ofrecido a sus clientes activos a través de las aquí mencionadas “asset centric criptotechnologies”, gracias a la implementación de Ripple Labs.

Todo esto por no citar otras propuestas de aplicación alejada del tema de la empresa y las finanzas como la de Permacoin, que propone un sistema de almacenamiento en la nube basado en P2P, que utilice los nodos funcionando mediante una “Proof of Retrievability” (PoR), dependiendo de la capacidad de almacenamiento de los nodos en vez de su capacidad de computación.

También son de destacar los conceptos de Smart Contracts, sistemas de crowdfunding y DAOs (Decentralized Autonomous Organizations), sistemas de votación en base a reglas predeterminadas, todos basados en el uso del blockchain, ofrecidos por Ethereum.

Por otro lado, la startup Ascribe o la nueva firma ilibrium de Hollywood, desarrollan aplicaciones del blockchain para la protección de la propiedad intelectual de organizaciones, artistas e individuos, que no permiten copiar el contenido sin autorización o permiten rastrear cuando un archivo se ha copiado o cambiado de manos, permitiendo así tomar acciones al respecto (Lombardo 2015; Biggs 2015).

Tomando distancia respecto de los aspectos administrativos y financieros, son relevantes las investigaciones en curso acerca del posible uso del blockchain en el ámbito energético por la posibilidad, por ahora teórica, de utilizarlo en el futuro para rastrear los flujos de electrones en la red eléctrica, del mismo modo que sucede ahora con los activos o el valor monetario en el bitcoin y de autenticar “transacciones energéticas”.

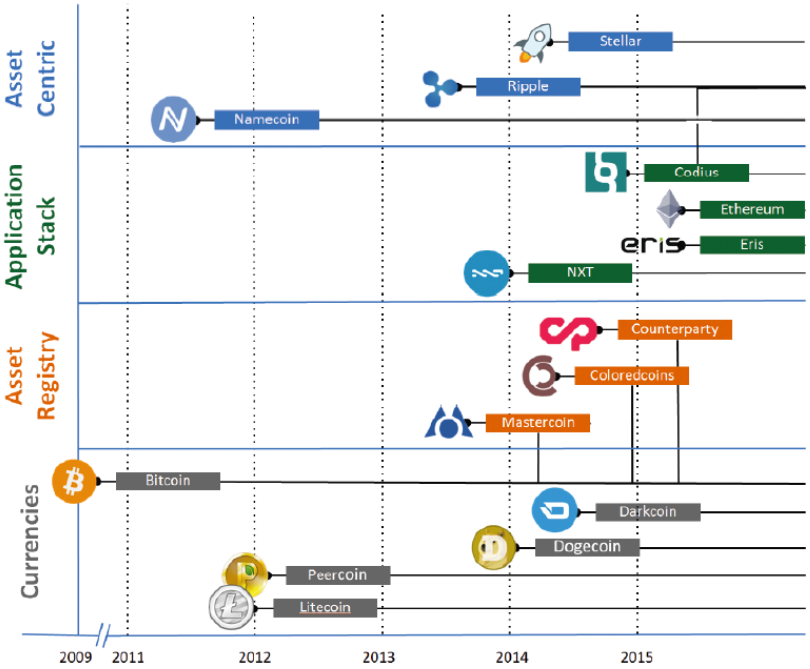
Otro ejemplo es la aplicación en el mundo del internet de las cosas, que han desarrollado IBM y Samsung a partir del software para autenticación de Smart Contracts de Ethereum, llamada ADEPT, para permitir que los dispositivos eléctricos de una vivienda puedan comunicarse, facilitando su estado y optimizando su funcionamiento (Lacey 2016).

Relacionado también con el blockchain y el internet de las cosas, una startup llamada Filament, ha desarrollado un paquete de sensores llamado Tap, que funcionan a partir de una serie de protocolos como el de Bitcoin, Jose, TMesh, Telehash, o BitTorrent y que pretenden permitirles almacenar contratos en los sensores sin conexión, hasta durante un año, e intercambiar información entre Taps, relativa a granjas, pozos petrolíferos o minas, hasta a 9 millas de distancia entre ellos, por unos 25$ de precio cada sensor, con importantes posibilidades a la hora de recabar la información o almacenarla, por ejemplo en la nube (Higginbotham 2015).

Existen una plétora de experimentos y eventos de gran potencial, relacionados, como el acuerdo entre Factom y HealthNautica para asegurar y autenticar las facturas, quejas, informes médicos, … en una base de datos distribuida como la de bitcoin (Suberg 2015).

Todas estas utilidades de la tecnología en que se basan las criptomonedas, son susceptibles de implementarse para mejorar la eficiencia de muchas empresas y transformar sectores enteros.

Figura 3.6.: Las cuatro categorías de desarrollo de las criptotecnologías



Fuente: EBA working group on electronic and alternative payments 2015

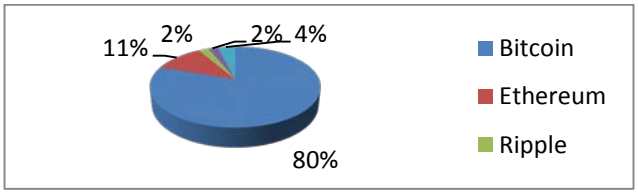
4. ECONOMÍA Y MERCADO DE LAS CRIPTOMONEDAS

4.1. ÍNDICES Y PARÁMETROS A UTILIZAR EN EL ANÁLISIS DE LAS CRIPTODIVISAS COMO INVERSIÓN O MEDIO DE PAGO

En la industria de las criptomonedas, dada la actividad especulativa que ha llegado a desarrollarse por parte de usuarios a través de exchanges, minería,… y fácilmente localizables en la vasta cantidad de webs dedicadas a proporcionar información actualizada en relación con las criptodivisas, tal y como menciona Farell (2015), en cuyo trabajo nos hemos basado en gran medida para la redacción de éste apartado, se pueden distinguir tres indicadores relevantes de éxito, que son: capitalización en el mercado, número estimado de usuarios y volumen de transacciones en un determinado periodo de tiempo (generalmente diarias).

En lo relativo al primero, es el Bitcoin la criptodivisa que aún acapara la mayor capitalización de mercado, 6.416.595.845 $, que representa, frente al total de 8.086.612.014 $, un 79,3% (coinmarketcap.com, marzo 2016).

Figura 4.1.: Capitalización respecto del total de los coin más cotizados en en mayo de 2016.



Fuente: Elaboración propia a partir de los datos de coinmarketcap.com (Mayo 2016).

El número de usuarios, es imposible de obtener y la dificultad para identificar individuos concretos, a pesar de ser públicamente conocido el historial de transacciones, complica las estimaciones, habitualmente basadas en las wallets creadas dentro de las plataformas online más populares, teniendo siempre en cuenta que una persona puede tener varias. Además, esto es sólo representativo para el bitcoin. Sin embargo, el volumen de transacciones diarias, se puede obtener con exactitud, para cualquier criptomoneda.

Figura 4.2.: Evolución de la capitalización y volumen de transacciones diarias del bitcoin, los últimos años (59.976.400 $ a 25 de Marzo de 2016).

Fuente: coinmarketcap.com (Marzo 2016).

Otro parámetro interesante para evaluar el grado de uso como medio de cambio de las criptomonedas basadas en blockchain frente al uso especulativo, es el ratio que relaciona el volumen de transacciones ya citado, frente al volumen de adquisición del coin en exchanges. Las transferencias entre propietarios de coins, la adquisición de los propios coins, … son procesadas por la red, pero dentro de las entidades intermediarias como exchanges, processors, … se realizan operaciones en base a monedas fiat y otras desconocidas, en las operaciones de cambio e intermediación. A pesar de no poder comprender la extensión de la influencia de éste último tipo de operaciones, es probable que el blockchain reste importancia al volumen de transacciones con propósito de transferencias y comercio. Así, el crecimiento de éste ratio implicaría un mayor uso de la criptomoneda como medio de cambio y menor como medio especultativo y viceversa (Stephanie Lo y J. Christina Wang 2014).

La percepción pública juega un papel fundamental en la evolución de éstos indicadores de éxito de las criptomonedas, al basarse fundamentalmente en las leyes de la oferta y la demanda, es decir, el número de usuarios dispuestos a confiar e invertir en ellas. Así, podemos identificar grupos de condicionantes relevantes de su situación, que serán posteriormente abordados en detalle:

- Tecnología: los diferentes esquemas de protocolo presentan distintas problemáticas, y se relacionan con factores como el precio del suministro eléctrico, o la vulnerabilidad a ataques informáticos, según el grado de desarrollo de cada coin, circunstancias de gran peso en su aceptación.

- Economía: es de conocimiento general la relación con actividades ilegales de lavado de dinero, … que pesa sobre el Bitcoin en particular. Existen Bitcoin negros y esto es relevante, como también la actividad especulativa y a través de ésta las variaciones del valor de las monedas y otros parámetros económicos.

- Ecosistema: proveedores de servicios construidos en torno a las criptomonedas, y otros individuos u organizaciones interesados, generan promociones y las distribuyen gratuitamente o a cambio de comentarios en foros, … (faucets) para extender su uso y conocimiento por parte de los usuarios, obtener ingresos o visitas y el paso del tiempo hace que las criptodivisas establezcan entidades cada vez más dignas de confianza y regulación en su entorno, que, a su vez, favorecen el intercambio económico.

- Regulación: hay casos claros de influencia como el de Rusia, que prohíbe el uso de las criptomonedas, y la incertidumbre producida por la no aceptación como moneda o los cambios de regulación en los diferentes lugares, también afectan notoriamente a su evolución, aunque no exista el control de una autoridad concreta.

- Noticias: un ejemplo de la influencia de la prensa, aunque quizás no muy claro por coincidir con la variación del yuan respecto del dólar en la misma fecha, es el repunte del precio del bitcoin, entre el 8 y 9 de diciembre de 2015, coincidiendo con el falso desenmascaramiento de Satoshi Nakamoto (Rizzo 2015). Además, es notable la cantidad de páginas web y exchanges que proveen datos como los parámetros anteriormente explicados y su evolución en el tiempo.

4.2. FACTORES DE INFLUENCIA A NIVEL GENERAL Y ESPECÍFICO RESPECTO DE OTROS MEDIOS DE PAGO Y DE LA MONEDA FIAT

4.2.1. Tecnología: impacto en el aspecto económico de las criptodivisas

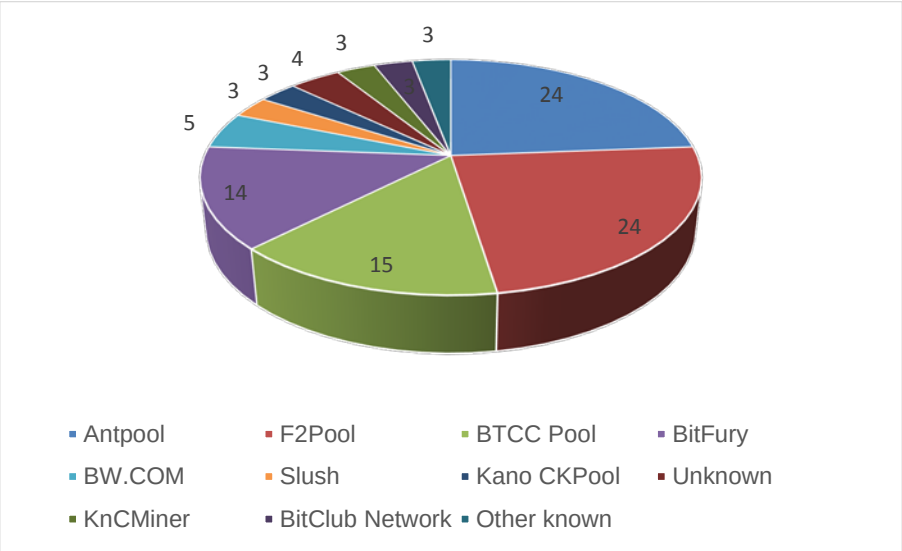
En el momento de redacción de éste trabajo, marzo 2016, existen 648 criptomonedas y 56 criptoactivos (coinmarketcap.com, 2016), si bien se basan en cuatro esquemas para el procesamiento de las transacciones mayoritarios (PoW, PoS, híbridos y basados en el "Problema de los Generales Bizantinos"). La situación no ha cambiado mucho respecto del 2015, cuando se redactó el artículo de Farell referenciado en la bibliografía y en el que se basa también, buena parte de éste apartado.

Para validar la autenticidad y evitar el doble gasto, como hemos visto, los mineros han de consumir recursos, que pueden ser una combinación de electricidad y tiempo o una cesión temporal de "coinage". La recompensa de los mineros es, por ejemplo, en el caso del bitcoin, la creación de nuevos coin asociados al bloque comprobado, que se ve limitada en el tiempo por haber un límite superior de diseño de 21 millones de BTC y la recepción de tasas por verificar transacciones de los usuarios, que fue pensada como sustento futuro del nivel de seguridad de la red. Todo esto, así como la variación de la dificultad de cómputo en el caso de los sistemas PoW, ha de ser tenido en cuenta a la hora de iniciar una inversión de minería y es importante de cara a la sostenibilidad de las redes.

Relacionado con esto y también en cuanto al bitcoin, existe rechazo entre ciertos economistas por la supuesta tendencia deflacionario del mismo, que se podría deducir del posible impulso acumulativo de los que los poseen tras alcanzarse el umbral máximo de los 21 millones.

Retomando el concepto de prueba de trabajo (PoW), se trata, como hemos dicho antes, de la resolución de funciones de verificación vinculadas a hashes, de dificultad determinante, cuyo éxito depende linealmente de la potencia de procesamiento de CPU empleada y del gasto de electricidad y tiempo. Su introducción en el bitcoin ha producido una carrera en el desarrollo de hardware por parte de los mineros, pasándose del uso de CPUs (Central Processing Units) al de GPUs (Graphics Processing Units), FPGAs (Field-Progammable Gate Array) y finalmente ASICs (Application Specific Integrated Circuits). Recientemente han surgido el MaaS (Mining as a Service), que se basa en grandes centros de computación rentando su capacidad a los mineros, además de las Mining Pools, aparecidas con la reducción de los beneficios de los mineros por separado, que deciden aunar esfuerzos generando cada bloque de forma distribuida y compartiendo los beneficios (los esquemas de actuación para evitar el fraude son variados: BPM o slush's pools, PPS o Pay per Share, Luke Jr's, P2Pool,…). Todo esto hace temer sobre los principios de descentralización de las criptomonedas y especialmente el Bitcoin, que se ven comprometidos por la aparición de economías de escala, encontrándose la minería de Bitcoins concentrada en poder de unas pocas Pools, que comienzan a localizarse en determinadas regiones geográficas.

Figura 4.3.: Distribución de las tasas de hash entre los Pools de minería de Bitcoin de mayor tamaño.



Fuente: Elaboración propia a partir de los datos de blockchain.info (25 Marzo 2016)

La prueba de tenencia (PoS) surge posteriormente a PoW y se basa en la posesión de la propia criptomoneda como recurso escaso, dependiendo el éxito al verificar las transacciones (y recibir la recompensa, transaction fees o recompensas de inicio de minado), de las criptomonedas poseídas por el minero en cuestión, en vez de su capacidad de cómputo, siendo necesario poseer más de la mitad de coin para comprometer la seguridad de la red. Generalmente no tienen un límite superior en su cantidad total y resultan inflacionarios. Otro problema es la distribución inicial de la criptomoneda, frente a PoW, causa de los abundantes fraudes por auto asignarse los creadores, la mayor parte de las mismas, haciendo más sencillo, al menos en su momento de creación, al ataque del 51%.

Ante la ineficiencia energética a largo plazo de los sistemas PoW y el problema de la distribución en el inicio, de los PoS, surgieron esquemas que combinan el funcionamiento como PoW en sus inicios y PoS más adelante. El primer ejemplo, que coincide con la primera aparición del PoS, es el PPCoin.

Otra solución a los problemas de PoW y PoS, son los sistemas basados en soluciones al “Problema de los Generales Bizantinos”, con opciones como Ripple y Stellar. La transacción debe ser aceptada por un 80% de los nodos para alcanzar consenso, siendo más robusto, rápido y eficiente desde el punto de vista energético, según Farell (2015), que PoW, y resultando necesario un ataque del 80% para corromper la seguridad de la red (con los matices señalados en el apartado correspondiente). En el caso de Ripple o Hyperledger, además, se requiere que los nodos tengan identidades legales y permisos para validar transacciones, algo que en el caso del Bitcoin, por ejemplo, no ocurre, si bien, estaríamos hablando de sistemas centralizados y basados en la confianza, sin los beneficios que supone la descentralización garantizada por las otras opciones.

A continuación, volviendo a los sistemas PoW y PoS, se presentan los problemas y ataques a los que son, o han sido vulnerables (BitFury Group, 2015), de los que podemos deducir que el PoW y el PoS delegado (como en Tindermint o BitShare) son más seguros en lo relativo a la red, si bien hay una importante polémica al respecto, encontrándose los sistemas híbridos como Ethereum, en plena emergencia en el momento de la redacción de éste trabajo:

- Nada en posesión: en un sistema estrictamente PoS, tras un fork, el comportamiento racional es prolongar ambas ramas. En PoW, esto no se contempla, pues dividir los esfuerzos disminuye las probabilidades de encontrar un bloque en cada una, cosa que no ocurre con PoS. Apoyándose en los forks, los ataques de doble gasto tienen éxito con mayor facilidad y los usuarios con más coins o si los mismos están repartidos entre muchos usuarios y unen esfuerzos, contribuirán aún más al mismo. Frente a esto, los esquemas de PoS delegado pretenden proporcionar una solución, dado que los mineros ceden como garantía, una cantidad de coins que correría el riesgo de desaparecer como castigo en caso de ataque.

- Problema de la distribución inicial: siempre existe la preocupación de que los propietarios iniciales de coins no tengan suficientes incentivos para distribuir las monedas, que contribuyen a su riqueza. En un sistema PoW, los propietarios deben mejorar su velocidad de hardware y mantener sus esfuerzos para mantener o cambiar de posición, en la misma medida que el resto de los mineros, pero para PoS no existe tal restricción y muchas de las criptomonedas utilizan un sistema de distribución inicial de la riqueza, como Peercoin, que utiliza PoW en su etapa inicial.

- Ataque de largo alcance: cabe la posibilidad, frente a la dificultad existente en PoW, de que un minero con suficiente poder de computación trate de generar una cadena de bloques alternativa a partir del primer bloque. Para evitarlo, los sistemas suelen definir una máxima profundidad de división de ramas, que permite discernir a los nodos conectados, entre las ramas válidas. Sin embargo, los nuevos nodos deben descargar el blockchain desde algún repositorio de confianza, lo que convertiría el sistema en semicentralizado (subjetividad débil requiriéndose una confianza parcial en ciertos agentes, combinada con la seguridad criptográfica, frente a la objetividad del PoW), aunque ésta casuística es la más extendida en éste tipo de sistemas.

- Ataque de soborno (doble gasto en PoS): el atacante realiza un pago de bienes o servicios, espera a que el comerciante considere la transacción confirmada y ofrece recompensa por minar en ramas truncadas distintas de la del pago, no perdiendo nada los involucrados y siendo rentable la acción siempre que la cuantía de los sobornos fuera menor que la del pago. Esto se ve solucionado en PoW, donde se debería sobornar a la mayoría de mineros a un precio muy alto, por gastar aquellos, además, recursos de computación (también se soluciona en sistemas de PoS delegado).

- Ataque de acumulación de coinage: al principio de la red de Peercoin, por ejemplo, un atacante podía esperar para acumular coinage y posibilidades de realizar ataques de doble gasto, … con mayores posibilidades de éxito. Posteriormente, se limitó el tiempo de acumulación de coinage a 2 meses, lo que, sin embargo, también limita las ventajas de usar coinage en vez de simplemente PoS.

- Ataque de precomputación: es algo de lo que está protegido el PoW por su dificultad de computación incrementada y también el PoS delegado por la no influencia de las propiedades del bloque más nuevo, en una secuencia de firmantes de bloques. Este ataque consiste en aprovechar, por un minero con mayor capacidad de cómputo, la posibilidad de influenciar el hash de un bloque, para poder minar el siguiente añadiendo nuevas transacciones al primero. Así, puede generar una cadena de bloques más larga para conseguir

tasas que no le corresponden y generar dobles gastos y sobrescribir la parte del blockchain correspondiente.

- Ataques DoS: se trata de perjudicar el funcionamiento normal de la red inundándola, por ejemplo, de transacciones de pequeño valor. Existen ejemplos de éste tipo de ataque a la red de bitcoin, por ejemplo, en julio de 2015.

- Ataques Sybil: el atacante crea un cierto número de nodos que se comportan de un modo perjudicial para la red. Tanto en éste caso como en el anterior, no hay motivo apoyado en los fundamentos de los sistemas, por el cual afirmar que el PoS sea menos susceptible a ellos que el PoW.

- Minado egoísta: propio del PoW, consiste en la revelación selectiva de bloques minados sucesivamente por el atacante e introducidos de una vez, para malgastar los recursos de mineros honestos, aunque no está demostrado que haya ocurrido en bitcoin e incluso hay quien defiende que está basado en hipótesis erróneas.

Para protegerse del doble gasto, los comerciantes habitualmente esperan cierto número de bloques por encima del continente de la transacción para aceptar como confirmada la misma y utilizan mecanismos para disminuir el riesgo de estos problemas, como desarrollaremos más adelante.

4.2.2. Economía y alcance: postura de bancos y otras empresas y recomendaciones para la actividad comercial con criptodivisas.

Numerosos fabricantes, comerciantes y plataformas se han sumado los últimos años a la aceptación de bitcoin como forma de pago, algunos tan importantes como Amazon, Ebay, TigerDirect, Overstock, … aunque desde el punto de vista del consumidor existen marketplaces y servicios intermediarios como Purse.io, o tarjetas Visa recargables con criptodivisa (SHIFT), que permiten a los usuarios conseguir cualquier producto. Pese a todo, la pequeña cantidad de usuarios de la red, en comparación con los de medios tradicionales, hace suponer que el principal motivo de su aceptación sea como estrategia de marketing, para reforzar o mantener una imagen innovadora.

Relacionado con el posible uso en el ámbito comercial y a pesar de la postura parcial de las entidades financieras, comentaremos a continuación cómo el Banco de Boston explica la correspondencia de los atributos del Bitcoin con las características de una moneda, en el artículo “Bitcoin as Money?” de Stephanie Lo y J. Christina Wang (2014) y añadiremos algunos comentarios sobre las posibles formas de utilizarlo en empresas y recomendaciones básicas que, añadidas a las del apartado siguiente, constituyen un conjunto de buenas prácticas para usar criptodivisas tanto desde la posición de las empresas como desde la de los consumidores.

En lo relativo al papel de unidad de cambio, los comerciantes han de considerar su gran volatilidad en el periodo de unas horas, que no existe para las monedas fiat como el dólar, pudiéndose estar realizando descuentos, con éste fundamento, a ser tenidos en cuenta. De hecho, los precios en éstas tiendas en línea, suelen publicarse en dólares y otra moneda además de en bitcoin. Una solución que minimiza el impacto de esto, es el uso de los procesadores de pago que cambian los bitcoin pagados por los clientes inmediatamente a dólares, que les son entregados a los comerciantes, manteniendo las tasas de cambio constantes durante un periodo dado de tiempo. Sus tasas varían ampliamente, si bien, podemos encontrarlas en torno al 1% en algunos de los más conocidos como Bitpay y Coinbase, como vemos en la figura, siendo interesante investigar, en caso de utilizar cualquier opción, consultando a los

responsables, si cargan a los clientes algún tipo de tasa adicional en las compras que pueda quedar oculta para el negocio y grave la transacción para el consumidor.

Figura 4.4.: Capturas de las tasas y modalidades ofrecidas por los procesadores de pago de bitcoin Coinbase y Bitpay respectivamente.

Fuentes: sitios web de Coinbase y Bitpay (Marzo 2016)

Otra problemática surge en torno a las devoluciones, dado que hay que calcular, por un lado, el importe que ha de ser retornado al cliente que ha pagado con bitcoin, con base a su valor en algún momento y realizar una nueva transacción con una tasa de cambio diferente. Así, los comerciantes que aceptan bitcoins, normalmente sólo permiten devoluciones a través de tarjetas regalo a gastar en la misma tienda.

Pese a todo, existe un ahorro para dichos negocios por las transacciones en bitcoin, derivado de la supresión de los costes relacionados con el proceso de pago, de entre el 1 y el 3%, fundamentalmente debidos al uso de tarjetas de crédito o medios tradicionales de pago online, o entre el 7 y 8%, a través de transmisores de dinero sin implicar cuentas bancarias (European Banking Authority 2014).

Por tanto, tasas de transacción son, en general y de momento, más beneficiosas a través del bitcoin, que de la moneda fiat para ambas partes, comerciante y comprador; y pese a que cada vez tardan más en confirmarse volviéndose necesaria la introducción de transaction fees para mejorar la velocidad de confirmación, también la velocidad de los pagos es más rápida, además de irreversible. Todo ello se debe a la eliminación de comisiones y trámites burocráticos como, los necesarios con las tarjetas, Paypal o los bancos, en el almacenamiento o movimientos de capital, algo se deja notar especialmente en transacciones internacionales o cuando se deben llevar a cabo cambios de divisa.

También debemos tener en cuenta, si nos decidimos por usar criptomonedas, las tasas cobradas por los exchanges o casas de cambio, que varían ampliamente según los casos. Además de las relacionadas con la transferencia bancaria o por tarjeta y del importe inicial a cambiar, hay que considerar las cobradas por el exchange en cada transacción, que suelen ser mucho menores al 1%, pero también las de depósito y de retirada de fondos, más importantes en general. También es interesante conocer la moneda fiat que utilizan el exchange o podríamos tener que lidiar con un coste adicional ligado al cambio de divisa correspondiente.

Figura 4.5.: Comparativa de las tasas y características de algunos de los exchanges más populares.

	Kraken	Bitstamp	Bitfinex
Valor del Bitcoin en el momento €	383.501	384,540	385,280
Tiempo para depósitos y retiradas	5/5 días mínimo	5/5 días mínimo	-
Tasas de transacción (sobre volumen mensual en USD)	0,16% ejecutor, 0,26% tomador (<50.000 USD)	0,25%(<20.000 USD)	0,1% ejecutor, 0,2% tomador (<500.000 USD)
Tasas de depósito	EUR en SEPA y criptodivisas gratis, 5 EUR transferencia bancaria (Excepto Ripple, 50 XRP)	Gratis criptodivisas y EUR en SEPA (0,05% transferencia internacional)	Gratis criptodivisas, 0,1% por transferencia bancaria, mínimo 20 USD
Tasas de retirada de fondo	0,09 EUR, 0.00050 BTC, Ξ0.00500 + 0.0050% ETH, …	0,9 EUR (10 USD mínimo)(0,09% internacional)	Gratis criptodivisas, 0,1% por transferencia bancaria, mínimo 20 USD (1% Express)
Criptodivisas soportadas	Bitcoin, Litecoin, Dogecoin, Namecoin, Ripple, Stellar, Ether	Bitcoin, Ripple	Bitcoin, Litecoin, Ethereum, TetherUSD
Moneda en que operan sus cuentas	EUR (Germany)	USD (UK)	USD

Fuentes: elaboración propia a partir de los sitios web de los exchanges (20 Abril 2016)

También se debe considerar que, pese a las desventajas señaladas de la propia criptomoneda en lo que a volatilidad se refiere y a la facilidad por parte de los comerciantes de acudir a exchanges o procesadores de pago para obtener o aceptar criptomonedas, existe la posibilidad de que realicen sus operaciones en bitcoins a través de un monedero propio, eliminando así, buena parte de todas éstas tasas. Además, las wallets online, como los depósitos proporcionados por los exchanges, son

sujeto de desconfianza por las personas que frecuentan las criptodivisas, por la ausencia de regulación y los antecedentes de fraudes y robos, que hacen necesario tomar precauciones en su elección como las que señalamos acerca de la información de aseguramiento ante robos y pérdidas, … en el apartado que versa sobre el ecosistema del bitcoin y sus problemas. Por tanto, es posible hacer frente a muchas de las amenazas allí citadas y evitar algunos de los costes referidos anteriormente por el uso de wallets, … tomando precauciones como (bitcoin.org 2016):

- Evitar los servicios online: porque son menos seguros y regulados, y más costosos.
- Utilizar pequeñas cantidades para uso diario: (como con un monedero convencional).
- Realizar copias de seguridad, completas y frecuentes: útiles frente a fallos humanos, de los dispositivos o robo.
- Encriptar las copias de seguridad conectadas a la red.
- Usar muchas ubicaciones seguras: para recuperar el acceso fácilmente en caso de pérdida de una de ellos (USB, CD, papeles, …)
- Encriptar el monedero y proteger el ordenador: contraseñas seguras, autenticación en dos pasos, utilizar equipos actualizados, identificar posibles vulnerabilidades, keyloggers, … que puedan exponer nuestros fondos.
- Utilizar un monedero offline para los ahorros: o almacenamiento en frío con las copias de seguridad y encriptación adecuados. Se puede:
    - Firmar transacciones fuera de línea: con dos ordenadores compartiendo partes del monedero, uno desconectado, para firmar transacciones (software tipo Armory), completo, y otro, conectado, puede crear transacciones sin firmar. Las transacciones se llevan del ordenador conectado al offline en USB para firmarlas.
    - Monederos físicos: no se puede instalar software y es fácil realizar copias de seguridad.
- Multi-firma: se encuentran en desarrollo aplicaciones de firma múltiple, para validar transacciones sólo si una serie de miembros firman la transacción.

En lo relativo a la característica de unidad de cuenta, la mayor desventaja de bitcoin vuelve a ser su volatilidad, que además lleva ligada el coste psicológico de ver fluctuar el precio de lo que van a comprar, por parte de los clientes que no saben ex ante, con precisión, lo que pagarán realmente por su adquisición, al ser la fluctuación de los precios de bienes y servicios, mucho menor en comparación. En el informe para el Banco de Boston comentado se señala también, que el control de suministro de moneda en función de las condiciones económicas que proporciona la moneda fiat, regulado por autoridades bancarias y gobiernos, es más seguro y menos sujeto a variaciones que asumir un suministro que varía por causas exógenas. Además, en base a la experiencia de casos anteriores como la crisis del euro de 2010-2011, mencionan que la adopción de una misma moneda en varios países distintos puede ser muy problemática.

En lo relativo al carácter de almacén de valor, de nuevo la volatilidad y la variedad de agentes e intereses que pueden influir en la moneda, y en éste caso, la aceptación de terceros como pago, está ligada a intermediarios como los mineros, exchanges y

otros, que ponen a disposición de los usuarios de la moneda los productos de comerciantes que aceptan el pago en otras monedas, frente a la moneda fiat que lo soluciona por la confianza en las entidades bancarias o los estados. Otro factor muy importante es la especulación en torno a la misma que genera burbujas, favoreciendo la volatilidad que hemos mencionado repetidamente, encontrándose esta especulación muy extendida para los altcoins, pero cuya posibilidad en el bitcoin por la acumulación de grandes cantidades es de dominio público y ha sido comentada en diferentes ocasiones, como es el caso de los gemelos Winklevoss en noviembre de 2013. Al principio del capítulo se tratan algunos parámetros utilizados para evaluar el éxito o la verdadera popularidad de las criptodivisas como medio de cambio, que nos pueden permitir evaluar el grado de especulación en torno a las mismas.

Todos estos inconvenientes ligados a la filosofía libertaria de las criptomonedas, descentralizadas, cuyos nodos pueden mantenerse en el anonimato y su vulnerabilidad actual ante la especulación, el fraude, ataques entre economías de distintos países,… hace que muchas compañías entre las que destacan los bancos, sean muy reacias a la aceptación de éste fenómeno, que, desde su origen, con el bitcoin, pretende robarles parte del control que mantienen sobre su negocio. Así, en informes como el de The Clearing House de 2014, se hace hincapié en desventajas relativas a la ausencia de regulación y al escaso grado de desarrollo de los ecosistemas en torno a las criptodivisas, que favorecen los fraudes, robos, …, explicados en otros apartados, cuyas verdaderas repercusiones negativas en la práctica, son previstas paulatinamente con el desarrollo del ecosistema, previamente a que aparezcan regulaciones gubernamentales apropiadas.

Es destacable la opinión sobre el tema de la European Banking Authority (EBA), reflejada en un informe de 2014, en el que se analizan los beneficios relativos a la reducción de los costes de transacción anteriormente mencionados, que arguye se basan en gran medida en la falta de regulación de las distintas entidades del ecosistema y argumenta que su beneficio se ve reducido para los estados de la Unión Europea (UE) dentro de la Single Euro Payments Area (SEPA), que iguala los costes de las transacciones nacionales e internacionales dentro del área, reduciendo parcialmente dicha ventaja comparativa, para las transacciones dentro de la UE. Valora también el tiempo de transacción como beneficioso, aunque en el caso de la SEPA y algunos otros países, se establece un máximo de un día para el crédito al receptor del pago, reduciéndose también ésta ventaja en tales lugares. Además, señala el crecimiento económico favorecido por la gran cantidad de nuevos negocios que han surgido en éstos ecosistemas, como el diseño de hardware especializado para minado, creación de oportunidades en el sector IT, … También alega que puede constituir un medio de cambio interesante en países en vías de desarrollo fuera de la Unión Europea en los que la moneda fiat o la regulación bancaria sea menos favorable, aunque señala como inconveniente que puede ser utilizada para saltarse las políticas de embargo y prohibiciones impuestas a individuos e instituciones, por gobiernos o instituciones internacionales. Como beneficios, alude a la seguridad de los datos personales por el grado de anonimato que garantizan criptodivisas como el bitcoin, además de la limitada interferencia por autoridades públicas, aspecto que despierta cierta polémica en cuanto al intervencionismo que deben tener los estados y los bancos sobre la economía.

Pese a los beneficios que contempla, dicho documento desarrolla en mayor medida los riesgos que acompañan a las criptodivisas, explicando unos 70, que coinciden los ya señalados en éste documento, además de algunos que tienen que ver con las relaciones de los agentes del ecosistema como los mineros, exchanges, … entre sí. A partir de aquellos, pone sobre la mesa una propuesta regulatoria a largo plazo, sugiriendo la posible inclusión de una autoridad destinada a su supervisión de carácter

no gubernamental, para mitigar los problemas de uso delictivo o por parte de criminales, la constitución de normativa para proteger a los consumidores y subsanar problemas como los mencionados en éste y otros apartados relativos a la transparencia de información, … A corto plazo, señala la necesidad de actuar sobre la normativa de lavado de dinero, … y de obligar a los nuevos servicios financieros aparecidos, a actuar conforme a una regulación básica de cara al consumidor, otros agentes, … avanzando en el sentido que contempla a largo plazo. También comenta la conveniencia de que las grandes entidades financieras trabajen por construir alternativas en el mercado, de criptodivisas fiables y competitivas frente a las existentes, descentralizadas y fuera de cualquier control.

Siguiendo éste último comentario de la EBA, en los últimos tiempos son notorios los esfuerzos de las entidades bancarias para incorporar elementos tecnológicos e ideas detrás de las criptomonedas en su infraestructura, en especial la de blockchain, tratando de desvincularse del propio bitcoin o alternativas de similar filosofía.

Así, destacan por ejemplo las acciones del Bank of New York Mellon, sobre el que hay noticias de su investigación acerca de la tecnología inherente al bitcoin, relativa al potencial de almacenamiento de transacciones, redes distribuidas, etc. acompañadas siempre del escepticismo de los economistas acerca de su carácter independiente respecto de los bancos (Boulton 2015).

También Oliver Bussmann, CIO del banco suizo UBS AG, está anunciando, también, su colaboración con startups y otras entidades, para introducir innovaciones tecnológicas relacionadas con el blockchain. Forma parte del R3 consortium, conformado por un importante número de bancos, que trabaja para aplicar tecnologías relacionadas, para dar lugar a libros mayores distribuidos en el contexto de los mercados financieros globales (King 2015), que, según un informe del Banco Santander, podrían ahorrar hasta 20.000 millones de dólares a los bancos, en costes de infraestructura, para el año 2022 (Simonite 2015).

Asimismo, el propio Banco Santander, en sus informes, ha mostrado interés en éste tipo de temas, destacando, por ejemplo, su inversión en Ripple Labs (Long 2015). Una ventaja importante, considerada por la banca en lo que respecta a las transacciones internacionales y defendida por el propio Ripple, es la posibilidad de realizarlas a un menor coste mediante la conversión intermedia a una criptodivisa, lo que aceleraría los trámites habituales (Simonite 2015).

Sin embargo, hay características de la tecnología que intentan imitar que no acaba de convencer a las entidades, destacando aspectos como la desconfianza en internet para ser soporte de transacciones o consideraciones de tipo comercial, como la mencionada por Richard Gendal Brown, director de tecnología de R3, de que "*Los clientes tienden a no querer que todo el mundo pueda ver sus transacciones financieras*" (Simonite 2015).

Pese a la opinión de los anteriores, hay auditorías, consultorías y otros servicios en el entorno de las entidades bancarias muy interesados en las oportunidades que las criptomonedas pueden brindar por sus características e innegables ventajas, abogando por ejemplo, en el caso de Deloitte (Deloitte 2015), por la creación de criptodivisa estatal desprovista de la naturaleza descentralizada del bitcoin, que podría ahorrar costes a entidades y gobiernos, si bien, a cambio de una importante inversión para adaptar y mantener la tecnología en funcionamiento. Otro caso análogo es el de Accenture, que también deja entrever su interés en el blockchain y sus aplicaciones relacionadas con Smart Contracts o libros mayores distribuidos, supuestamente sujeto de proyectos de sus Technology Labs para casos aplicados concretos (Accenture 2015).

Además, también algunas entidades bancarias han apostado por empresas y startups relacionadas con el propio bitcoin, como es el caso de Bankinter que invirtió en 2014 una cantidad desconocida en Coinffeine, empresa que posee software para el intercambio de bitcoin entre particulares sin intermediarios, o BBVA Ventures que se unió a las rondas de financiación de Coinbase en 2015, una importante empresa de servicios financieros relacionados con ésta criptomoneda, como procesador de pagos, exchange,…

El sector tecnológico es el que más oportunidades percibe en ésta novedad, con empresas como Microsoft, que a partir de su plataforma de almacenamiento en la nube, Azure, pretende crear una solución BaaS (Blockchain as a Service), que ya ha ofrecido como soporte para las nuevas experiencias del R3, dado que, como Marley Grey, estratega tecnológico para servicios financieros de la compañía, dice: *"Las infraestructuras a escala empresarial y de eficacia probada tendrán una importancia vital para esta infraestructura financiera que se tejerá durante los próximos años con el uso de cadenas de bloques"*. También IBM, Cisco e Intel colaboraron el último año, en un proyecto open-source relacionado con software de cadena de bloques, pero los mayores éxitos vienen de mano de startups, como hemos explicado antes, surgidas en los últimos tiempos y auxiliadas por entidades financieras para favorecer el desarrollo de los fundamentos de éste fenómeno y su explotación al servicio de las mismas, como es el caso de Ripple o Chain (Simonite 2015; Rizzo 2015).

Figura 4.6.: Comparación de las características de las criptodivisas con las de otros métodos de pago con dinero fíat.

Criptodivisas	Otros con dinero fiat
Regulación variable y volatilidad del valor	Estabilidad en regulación y valor
Coste psicológico de la volatilidad para el consumidor	Transacciones internacionales a un coste elevado
Dificultad en devoluciones	Elevadas comisiones cobradas por transacción al comerciante (tarjetas)
Irreversibilidad de los pagos	Posible cancelación de pagos
Reducidos costes de transacción	
Transacciones internacionales a muy bajo coste	

Fuente: Elaboración propia a partir de la información recabada en éste capítulo.

4.2.3. Ecosistema: funcionamiento, aplicaciones y agentes

Ya se han comentado brevemente conceptos como el de faucet y mencionado el de wallet, exchange o casa de cambio y procesador de pagos. Como ya se ha explicado, en torno a las criptomonedas se tiende a construir todo un ecosistema con numerosos y cambiantes elementos. Nos centraremos de nuevo en la más longeva y extendida, el bitcoin, para comentar los agentes y aplicaciones relacionados más importantes.

Las redes PoW son establecidas y mantenidas por los mineros, que validan las transacciones y las incorporan al blockchain en sus nodos de minería con el objeto de conseguir coins a cambio. Después, generalmente los ponen en circulación, vendiéndolos a los exchanges, que los hacen disponibles al público general.

Otro elemento de la red, que cumple el papel de cliente, son las wallets, en posesión de los consumidores y vendedores, que son un software, generalmente abierto y gratuito, que liga las direcciones de las cantidades de criptodivisa a sus propietarios y permite realizar transacciones entre los usuarios. Además, al asociar a sus usuarios con las direcciones, publican periódicamente en la red información que permite a los nodos desautorizar la incorporación de transacciones al blockchain realizadas por wallets diferentes. Existen múltiples tipologías, y variedad de opciones dentro de cada una, lo que podemos considerar una ventaja del carácter abierto del protocolo de la criptomoneda, además de ser un incentivo en la mejora de su seguridad. Mencionaremos las fundamentales (coindesk.com 2015):

- Desktop wallets: consiste la instalación del cliente en el ordenador. La oferta varía con opciones para diferentes SOs (Mac, Windows, …), existiendo unas más enfocadas en la seguridad, como Armory, otras en el anonimato, como Darkwallet, …

- Mobile wallets: cuando se desea pagar en una tienda física, pueden ser más interesantes. En forma de app, pueden desplazarse y existen opciones que utilizan NFC, igual que las wallet que ofrecen los bancos. No son un cliente bitcoin propiamente dicho, al no poder contener el blockchain completo, pero van acompañados de una verificación de pago simplificada, SPV, que descarga una porción del mismo y a partir de ahí, se apoya en el resto de la red para realizar las verificaciones. Hay multitud de aplicaciones para todos los SOs, destacando, por ejemplo, CoinPunk, que está adaptada a navegadores o Aegis Bitcoin Wallet, para smartwatches de Android.

- Online wallets: más adelante hablaremos de los exchanges, algunos de los cuales vienen acompañados de éste tipo de almacenamiento de criptomoneda. Tienen la ventaja de poder ser accedidos desde cualquier lugar e interactuar con otros tipos de wallet, pero la desventaja de la presencia del intermediario, con riesgos de comisiones, problemas de regulación y antecedentes de fraude, debiendo gestionar cuidadosamente, el usuario, sus operaciones.

- Hardware wallets: almacenes electrónicos de claves, como Trezor, USB Ledger, KeepKey, …

- Paper wallets: se pueden generar códigos QR o incluso apuntar en papel las claves privadas para evitar problemas del soporte electrónico.

Por otro lado, casos llamativos son los de empresas de servicios, componentes del ecosistema bitcoin, que ofrecen tarjetas de débito para operar en dicha criptomoneda, similares a las utilizadas con el dinero fiat, pero con referencia a depósitos online administrados bajo las condiciones de tales organismos (Cryptopay, Xapo,…), existiendo además, cajeros ATM que permiten extraer las cantidades monetarias en dinero físico si así se desea, si bien aún no se encuentran demasiado extendidos.

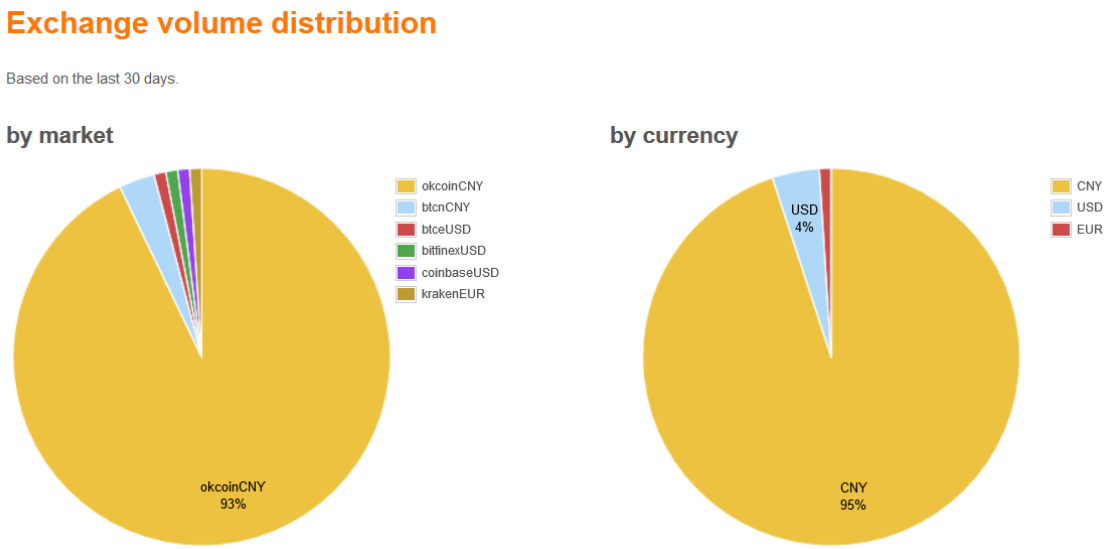
Otras entidades destacadas son los exchanges, plataformas online que permiten a los usuarios adquirir criptomonedas, en ocasiones de una gran variedad, a cambio de dinero fiat, contando a menudo con herramientas de análisis relacionadas con el habitual juego de la especulación. También suelen permitir el almacén de fondos,

aunque en éste caso el exchange mantiene su titularidad, en vez del usuario y pueden ofrecerse como procesadores de pagos para comerciantes.

Del mismo modo que las casas de cambio del dinero fiat como NASDAQ o NYSE, han evolucionado desde un mercado monopolístico hacia otro menos concentrado que permite una especialización mayor en función de las necesidades de los clientes (que pueden preferir más velocidad de operación, o menores costes de transacción, o …). Algunas comparativas y precauciones a tomar en su uso, se hallan reflejadas en el apartado correspondiente a la relación del bitcoin con distintos agentes económicos, de éste capítulo.

Atendiendo a la distribución de volúmenes entre exchanges durante los últimos 30 días, observamos que lo que más mueven son yuanes, debido a que buena parte de la actividad especulativa se desarrolla en China.

Figura 4.7.: Distribución del volumen de los exchanges por moneda y mercado (últimos 30 días)



Fuente: bitcoincharts.com (Abril 2016)

En cuanto a la aceptación de pagos, como hemos comentado ya, los comerciantes pueden recibirlos en una wallet propia o utilizar procesadores de pagos, intermediarios que facilitan los Bitcoin o el dinero fiat al comerciante, manteniendo tasas de cambio horarias o diarias fijas, para reducir los efectos negativos de la volatilidad. Referencias de algunas tasas aplicadas a comercios y precauciones a tomar, están reflejadas en el apartado correspondiente al papel en la economía de las criptomonedas, en éste mismo capítulo.

Pese a la estructura de servicios y actividades en torno a éste mundo, el escaso tiempo de vida, la falta de regulación detallada protegiendo al consumidor o la aparición de problemas técnicos combinados con el carácter descentralizado de las criptodivisas, favorecen la existencia de ciertos peligros (Consumer Financial Protection Bureau (CFPB) 2014) que son el motivo de que sus usuarios más estables hayan sido personas con cierta experiencia o conocimientos específicos en el medio, aunque las comunidades y la evolución de todo el ecosistema estén consiguiendo cambiar esto con el tiempo y hacerlas más accesibles a efectos prácticos para el público general (The Clearing House, 2014):

- Pérdida o robo: brechas de seguridad en wallets y exchanges pueden dar lugar a estos casos sin posibilidad, a menudo, de recuperarlas sin litigio, salvo por voluntad propia de los servicios. Es el caso de la quiebra de Mt. Gox, por un robo de 460 millones de dólares y 27 millones de sus cuentas bancarias (Mcmillan 2014). Así, aunque también existen vulnerabilidades en el uso indebido de medios de pago con dinero fiat, en computadores con problemas de seguridad, …, no existen seguros, como los provistos en EEUU por el FDIC, en el caso de fallo de los bancos o por el SIPC, en caso de quiebra de una firma, que cubran las actividades de los exchanges, ….

- Uso desautorizado: para cualquiera en conocimiento de nuestras claves privadas, es posible realizar transacciones con nuestros fondos sin que sean reversibles (lo que ocurre también con el dinero fiat en efectivo, siendo recomendable y posible en el caso de las criptomonedas, el cifrado de las claves privadas).

- Errores de procesamiento de transacciones: Si hay errores de funcionamiento o fallos en el acceso a las wallets, exchanges o los procesadores de pago, pueden no ser reversibles y el consumidor no tiene opción de recurso legal contra tales medios (aunque hay jurisdicciones en que ya empiezan a regular éstos servicios y hay antecedentes de procesos judiciales relacionados, en EEUU). Aquí, se nota una vez más la falta de regulación, pues, por ejemplo, una extensión de la CFPB, podría obligar a éstos servicios, como ya lo hace con medios de pago en moneda fiat, a posibilitar el cancelar las transferencias en un periodo de 30 minutos tras la solicitud de la misma y a contemplar otras medidas de protección al consumidor tanto en EEUU como fuera.

- Divulgación de fallos: los servicios citados no tienen obligación de compartir información relativa a problemas, casos de aseguramiento ante robos o pérdidas que afecten a los usuarios, fluctuaciones del valor de las criptomonedas, … Así golpea de nuevo, la falta de regulación, dejando a los consumidores a merced de este inconveniente, aunque la adopción de precauciones como las indicadas y la abundante información en la web, pueden reducir los riesgos en la práctica.

4.2.4. Regulación en el mundo y en España

Como se ha podido verificar en el artículo de Farell de 2015 y en el apartado correspondiente a legislación sobre monedas virtuales de la web de la “Library of Congress” de EEUU, que han vertebrado esta sección del trabajo, las criptomonedas no son aceptadas como medios oficiales de pago en ningún lugar del mundo, ni son consideradas como monedas propiamente dichas. Pese a ello, la postura de los diferentes estados es diversa, habiéndose regulado ya, en muchos de ellos, aspectos relevantes de su uso.

La postura de EEUU es permisiva y neutral, siendo contempladas las criptomonedas como propiedad de cara al pago de impuestos. Es el FINCEN, a nivel federal, quien ha realizado esfuerzos de regulación y ha estudiado cómo contemplar éstos nuevos elementos tecnológicos desde 2013, no considerando el uso individual, como Money Service Bussiness (MSB) pero sí los Exchanges y servicios de cambio, que deben respetar la normativa vigente al respecto, de 1970. Este es un importante paso en cuanto a la seguridad frente al fraude. Además, California, el estado con mayor actividad de criptomonedas, ha concedido estatus legal a las mismas en su jurisdicción y Nueva York, interesada en el fenómeno, comenzó a aplicar en 2015 nueva normativa acerca de su uso en comercios.

Australia, con el 7% de los usuarios de Bitcoin, también sigue las leyes de tasación de bienes y servicios (GST), desde 2013, considerándose aplicable a las transacciones de criptodivisa, a partir de 2014, la normativa relativa al trueque.

Canadá ha sido el primer país en desarrollar una normativa específica para la tributación de las criptomonedas, buscando minimizar los riesgos asociados de financiación de organizaciones terroristas y el lavado de dinero y monitorizando éste tipo de transacciones. El Banco de Canadá ha manifestado su deseo de que sea reconocido un mercado de monedas virtuales, si bien, actualmente, tan sólo valora las criptomonedas como una inversión, no como monedas.

En China, el Banco Central restringe el uso fuera de las instituciones financieras, dejando las criptomonedas para el ámbito privado o individual y recomienda a los ciudadanos utilizarlas como un bien (una “virtual commodity”), no como una moneda para realizar intercambios.

Por su parte, en Rusia, partiendo de la consideración del Banco de Rusia como facilitadoras del lavado de capitales y financiación terrorista, contemplada en una declaración de 2014, percibe como una actividad sospechosa el uso de las criptomonedas y una violación de las leyes federales que permiten la existencia de un solo Banco Central y moneda. Durante el mismo año se propusieron leyes sobre posibles castigos y multas, habiéndose cerrado a lo largo de 2015, diversos sitios web relacionados.

Otro caso llamativo es el de Islandia, que no las confiere estatus legal, y cuyo Banco advierte de que la adquisición de las mismas o el comercio fuera de sus fronteras con ellas, incumplirían el Icelandic Foreign Exchange Act.

En 2012, se analizó en el seno de la Unión Europea, la posible regulación por directivas ya existentes sobre dinero electrónico (2009) y medios de pago (2007), de las criptomonedas, aunque se concluyó que se salían de lo estipulado en dicha normativa. Desde entonces destacan las advertencias a los consumidores por parte de la European Banking Authority (EBA), acerca de los peligros de realizar transacciones mediante criptomonedas, la desprotección legal de las mismas y los compromisos fiscales que derivan de su posesión.

En España no existe regulación al respecto, aunque podrían considerarse como bienes digitales según el Código Civil y las transacciones, ajustarse a las operaciones de trueque contempladas en el mismo, requiriéndose a los comerciantes que reciban pagos en criptomonedas, que generen facturas con el valor de los impuestos añadidos en euros; si bien, la resolución del TJCE mencionada más adelante, podría abrir un debate institucional que culmine con otras consideraciones acerca del carácter jurídico del bitcoin.

En el caso de España, ha tenido lugar también cierta actividad parlamentaria que apuesta por mayor regularización relativa al bitcoin, como es ejemplo la intervención de Rosa María Díez del grupo político UPyD, de enero de 2015. Se ha de mencionar también que existen ya diversos casos y sentencias que involucran la criptodivisa del bitcoin en alguna medida, por tener características especialmente atractivas para delincuentes y criminales.

Relacionado con ésta última consideración tenemos a nivel europeo el caso Skatteverket contra David Hedqvist, con sentencia del 22 octubre 2015, que presenta dudas acerca de la consideración del bitcoin como moneda o medio de pago, pues si bien no es considerado como tal a ojos del BCE y los gobiernos de los estados miembros, en ésta sentencia el Tribunal de Justicia de la Unión Europea (TJCE) lo valora de otra manera, al reconocerse la exención de IVA en el cambio de bitcoins.

A éste respecto se abren interrogantes con consecuencias importantes, como el relativo a la afección de las leyes de prevención del blanqueo de capitales o de lucha contra el fraude fiscal, que limitarían el importe máximo de las transacciones a 2.500€, como sucede con el efectivo, habiendo declarado lo siguiente el Gobierno, ante la cuestión de Anchuelo Greco Álvaro, portavoz del grupo UPyD ante el Congreso, dejando la respuesta definitiva en manos de unas instituciones europeas que aún no terminan de definirse al respecto:

> *"En relación con la normativa aplicable, se puede destacar que, con la finalidad de luchar contra el fraude fiscal en el anonimato de los medios de pago, se establecieron limitaciones a los pagos en efectivo por el artículo 7 de la Ley 7/2012, de 29 de octubre, de modificación de la normativa tributaria y presupuestaria y de adecuación de la normativa financiera para la intensificación de las actuaciones en la prevención y lucha contra el fraude. Esta norma financiera establece que no pueden pagarse en efectivo las operaciones, en las que alguna de las partes intervinientes actúe en calidad de empresario o profesional, con un importe igual o superior a 2.500 euros o su contravalor en moneda extranjera. En caso de incumplirse esta prohibición, se establece una elevada sanción -el 25 por ciento de lo satisfecho en efectivo- con lo que se desincentivan estos pagos cuando sobrepasan determinado umbral.*
>
> *Esta norma establece que se entenderá por efectivo los medios de pago definidos en el artículo 34.2 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, que comprende, entre otros, "Cualquier otro medio físico, incluidos los electrónicos, concebido para ser utilizado como medio de pago al portador".*
>
> *En el caso de que las autoridades monetarias y financieras consideren que el "bitcoin" es un medio electrónico concebido para ser utilizado como medio de pago al portador, serían de aplicación las limitaciones a los pagos en efectivo".*

Así se puede deducir que el principal factor relevante, relativo a la regulación del bitcoin (valorado como criptodivisa más extendida) y el desempeño de los diferentes servicios relacionados con su funcionamiento y existencia, es la incertidumbre e indecisión de las autoridades al respecto, que influyen negativamente en cuanto a su aceptación social y el desarrollo de negocios asociados al mismo, así como su estabilidad como moneda.

4.3. POSIBLES ESCENARIOS FUTUROS DE LA CRIPTOMONEDA

Se pueden pronosticar diferentes escenarios relativos al desarrollo futuro de las criptodivisas y las tecnologías en que se apoyan, y uno de los aspectos más interesantes, ligado a su nacimiento como aplicación en el bitcoin, es la relación con los bancos y PSPs convencionales. Así se distinguen cuatro casos (EBA Group of Work on Electronic and Alternative Payments, 2015):

- Creación de una criptoeconomía separada con sus propios agentes.
- PSPs compiten entre ellos por posicionarse como desarrolladores de aplicaciones sobre criptotecnologías.
- Los PSPs colaboran con las comunidades entorno a las criptotecnologías asociándose en áreas concretas de interés.
- Los PSPs y las comunidades entorno a las criptotecnologías colaboran y además se integran con éxito.

Al respecto, podemos ver que el primer caso es el que se ha dado durante los últimos años en el mercado de las criptodivisas, y el tercero es similar al actual, en el que múltiples entidades bancarias han estado estableciendo acuerdos para colaborar en el

desarrollo de mejores esquemas aplicados a su industria. Sin embargo, hay que tener en cuenta que comunidades como la del bitcoin, tan sólo dan pie al primer escenario, al abogar por la descentralización más pura al pretender conseguir un, tal como menciona Satoshi Nakamoto en la conclusión del artículo que originó el nacimiento de la criptodivisa:

> "system for electronic transactions without relying on trust."
>
> "sistema para transacciones electrónicas que no se basa en la confianza."

Pese a todo, hay diversos retos que el esquema PoW debe enfrentar, al incrementarse la escala del sistema y la alternativa, el Ripple, que aporta soluciones y está respaldada por el R3, ocupa actualmente la tercera posición en capitalización, detrás de Bitcoin y Ethereum, que también aboga por un esquema descentralizado (PoS/PoW). Así, depende de cómo enfrenten las dos últimas comunidades, que cuentan con la mayor cuota de mercado en el mundo de las criptodivisas, los retos sobre la escalabilidad del PoW, el hecho de que evolucionemos hacia un fututo con una economía más o menos centralizada.

5. CASOS DE ESTUDIO

5.1. DISEÑO DE LAS ENTREVISTAS

Aquí, se considerarán sólo las soluciones relativas al bitcoin, por ser la criptodivisa más utilizada, habiéndose intentado recabar información de empresas que lo aceptan como medio de pago, para sacar conclusiones acerca de su interés como tal.

Existen empresas, como Purse, que funcionan proveyendo a los consumidores de medios para operar con bitcoin y criptomonedas, en tiendas online que no las aceptan por sí mismas y también están presentes en el mercado con este fin, tarjetas de débito, recargables con distintas monedas y criptomonedas, como Shift, susceptibles de ser utilizadas en cualquier establecimiento que acepte tarjetas. Sin embargo, aquí se excluyen esos casos para conseguir una mayor fidelidad a los objetivos del trabajo, vinculado al papel de la criptodivisa en el mundo empresarial.

Así, al ser más fácilmente localizables que los usuarios de las criptomonedas y no estar especialmente interesadas en su éxito o fracaso por haber realizado inversiones directamente relacionadas con ellas, se ha realizado un estudio exploratorio aleatorio, con un cierto sesgo explicado después, mediante entrevistas estructuradas breves de preguntas, en su mayoría, abiertas, dirigidas a distintos negocios que han decidido aceptar éste tipo de pagos. Los modelos se recogen en el Anejo I, y a través de las cuestiones allí reflejadas se ha tratado de obtener una idea sobre la operativa en cuanto a las operaciones con bitcoin que utilizan las empresas, objetivos al tomar la decisión de aceptarlo y resultados de la misma, gracias a la información que han compartido con nosotros.

Se pueden encontrar en la red variados ejemplos de sitios como Bitstuff, que pretenden constituir sitios de intercambio de objetos de segunda mano a través de bitcoin, o mercados que se centran en el comercio exclusivo en éste tipo de criptodivisa, que no se incluyen entre los entrevistados por buscarse conocer los beneficios reales de su uso de forma objetiva y la comparación con los métodos de pago tradicionales.

De ésta forma se ha optado por un cierto sesgo hacia empresas relacionadas con el mundo digital, como proveedores de alojamiento web, de nombres de dominio, de VPN, …; y sobre todo hacia pequeñas y medianas empresas que lo han adoptado, por estimar el autor que se lograría una mayor cantidad de información al respecto y se podrían alcanzar conclusiones más interesantes acerca del interés de su uso en la práctica, correspondiéndose las respuestas con casos de tiendas, hoteles, restaurantes, gabinetes de abogados, … que han optado por ésta iniciativa.

Se han enviado 40 entrevistas, que han respondido 11 empresas, señaladas en el Anejo II. En cuanto a las preguntas realizadas, se han hecho 2 formularios diferentes en inglés y en español, realizándose el segundo con el fin de aclarar mejor las cuestiones, por si las mismas resultaban difíciles de comprender o responder con celeridad, para el entrevistado. En el apartado de respuestas, éstas se hallan ordenadas según las dos fases correspondientes a las dos iteraciones del ciclo de ejecución y diseño de las entrevistas que se expone en la figura 5.1.

En cuanto a las preguntas realizadas se ha valorado un número de 10, por resultar amigable a la vista y lo suficientemente corto para incentivar al receptor a responder, resaltándose cinco de ellas respecto del resto, por ser las más relevantes y englobarse las demás dentro del aspecto que trata cada una de las primeras.

La información que se pretendía conseguir se refiere, en concreto, al objetivo de las empresas al aceptar bitcoin como medio de pago, la ventaja comercial que ha supuesto dicha medida, la ventaja en cuanto a ahorro de costes, qué método utilizan para recibir los pagos en criptodivisa, la fecha en la que tomaron la decisión de utilizar criptomonedas, y el hecho de si operan con sus proveedores en criptodivisa o no. Así, la mayor parte de la información obtenida es cualitativa, a partir de la cual se pretende obtener conclusiones en cuanto a la operativa e interés de la medida en cada caso.

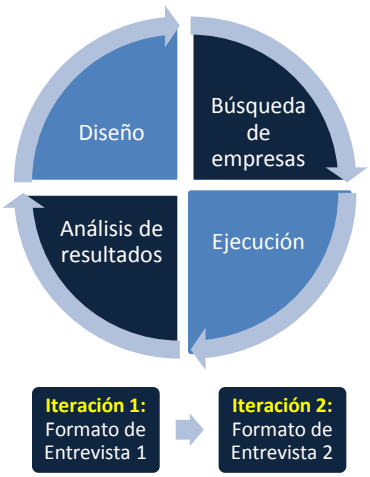
5.2. CONCLUSIONES DEL ESTUDIO

Podemos destacar de entre toda la información recabada una conclusión importante. Se puede dividir a los entrevistados en dos grupos, uno que ha dejado de aceptar bitcoin como medio de pago y que lo mantuvo entre 2012 y 2014 aproximadamente, por considerar que era una moda pasajera susceptible de mejorar su imagen y atraer clientes, que declaran haber tenido unos ingresos prácticamente nulos en dicha criptodivisa y otro que lo ha mantenido durante más tiempo, por tener más clientes interesados, lo que tal vez se encuentre vinculado con el desarrollo de los negocios en otros países o el contacto con público foráneo interesado en sus servicios.

Sin embargo, acerca de la eficiencia en costes no se puede sacar ninguna conclusión. Hay dos casos que dicen no haber obtenido ningún ahorro del uso del bitcoin frente a otros medios de pago, aunque uno es un restaurante-coctelería que probablemente reciba la mayoría de sus ingresos en efectivo y el otro afirma no haber recibido ningún cliente que haya optado por el uso de la criptomoneda. Por otro lado, tenemos una compañía dedicada a inversiones de capital riesgo en empresas relacionadas con el bitcoin, que afirma que el uso de bitcoin significa un 5% de ahorro para su actividad, otra que sólo ha realizado una venta pagada mediante bitcoin, que afirma que significó un 1% adicional de beneficio respecto de las operaciones habituales, otra relacionada con la venta de té que subraya un ahorro del 3% frente a los pagos con tarjeta y especial interés en transacciones internacionales y por último, otro negocio estadounidense, relacionado con el mundo de los videojuegos, que afirma que obtiene un ahorro de entorno al 3,5% frente a las tarjetas, lo que significa unos 0,9$ adicionales de beneficio por transacción, siendo frecuentada por aproximadamente, un cliente semanal interesado en utilizar éste medio de pago.

En cuanto a los métodos utilizados para recibir los pagos, destacan en general los procesadores de pagos, en especial Bitpay, Coinbase y BTCfacil, probablemente porque, como señala la empresa de videojuegos ateriormente citada, JJGames, que inicialmente utilizaba un sistema propio, eran más vulnerables ante errores irreversibles de la red. Tres empresas operan directamente en criptomonedas de entre las encuestadas y destaca la información proporcionada por Tealet al respecto, que afirma tener un sistema propio para aceptar pagos en Litecoin y declara poseer proveedores foráneos a los que paga mediante bitcoin a través de Align Commerce, llegando los pagos a su destino en la moneda local y consiguiendo una menor comisión por cambio de divisa que recurriendo a las entidades bancarias tradicionales.

Figura 5.1.: Proceso retroalimentado de ejecución y diseño de las entrevistas



Fuente: Elaboración propia

Figura 5.2.: Tabla resumen de datos sobre las entrevistas

Nº de entrevistados: 40	**Nº de respuestas**: 11
Objetivo comercial: 4	
Objetivo eficiencia: 1	
Objetivo compromiso social: 2	
Afluencia mensual de clientes interesados:	1 (1), 2 (1), 5 (1), Menos de 1 (6)
Ahorro estimado medio:	3,1% (4)
Métodos utilizados:	Coinbase(1), Bitpay(2), BTCFacil(1) y wallet propia(3)
Operaciones con proveedores:	2
Dejaron de operar con bitcoin	3

Fuente: Elaboración propia a partir de la información recabada

6. VENTAJAS Y DESVENTAJAS: APLICACIONES E INTERÉS EN EL ÁMBITO DE LA EMPRESA

6.1. EVALUACIÓN SOBRE LOS DISTINTOS TIPOS DE CRIPTODIVISA

En la siguiente tabla se refleja un resumen comparativo de las características más importantes relativas a los diferentes tipos de criptomoneda:

Figura 6.1.: Resumen comparativo de los distintos esquemas de criptodivisa

PoW (ej. Bitcoin):	PoS-PoW/PoS (ej. Peercoin)	Byzantine Agreement (ej. Ripple):
Carácter completamente descentralizado.	Reparto inicial centralizado o comienzo con PoW.	Fruto de acuerdos entre entidades financieras (centralizado y basado en la confianza).
Incremento del tamaño del blockchain en el largo plazo (también lo tienen los otros sistemas, aunque aquí se hace más evidente por su mayor desarrollo y su carácter descentralizados).	Repositorios de referencia del blockchain para evitar forks (factor de centralización adicional).	Menor tolerancia de fallos y mayor eficiencia energética
Tendencia deflacionaria (acumulación).	Tendencia inflacionaria habitualmente.	Mayor integración en el sistema económico y legal actual, tecnología en manos de proveedores de servicios
Ineficiencia energética.	Eficiencia energética.	
Peligro de economías de escala y concentración geográfica.	Mayores probabilidades de problemas de seguridad frente al doble gasto.	
Open Source y comunidad que lo mantiene de facto.	Open Source y comunidades que los mantienen de facto.	

Fuente: Elaboración propia en base al conjunto de documentos citados en la bibliografía

Teniendo en cuenta lo que ya hemos mencionado sobre las criptodivisas, es destacable por un lado, el carácter centralizado y basado en la confianza de los esquemas apoyados en el “Problema de los Generales Bizantinos”, que los alejan de nuestra definición de criptomoneda e interés como tal, pese a que parecen la apuesta de las entidades financieras en respuesta al resto y quizás sirvan en el tiempo, para mejorar su competitividad en factores como los mayores costes de las transacciones nacionales e internacionales, frente a los esquemas descentralizados.

Entrando en comentarios sobre las criptomonedas propiamente dichas, el bitcoin es la más utilizada y extendida en muchos aspectos, si bien se enfrenta a algunos problemas técnicos de cara al futuro, que su comunidad deberá resolver, como la concentración geográfica, la creación de economías de escala en el ámbito de la minería, el crecimiento del blockchain en tamaño con el tiempo (en éste momento de unos 66GB) y la probable aparición de la computación cuántica que antes o después exigirá el reajuste de los algoritmos criptográficos para mantener la seguridad de la red. Una posible solución para los más urgentes de estos contratiempos podría venir de mano del esquema PoS, como proponen algunos defensores de éste último tipo de protocolo, si bien buena parte de los problemas relacionados con su seguridad, que lo han hecho depender de una mayor centralización, motivados probablemente por su juventud, hacen dudar sobre la buena influencia de éste cambio. A pesar de esto, la segunda criptodivisa en el momento, después de bitcoin es Ethereum, un esquema combinado de PoW y PoS, enfocado en la implementación de Smart Contracts, realizados para ejecutar diversos servicios como intercambios financieros, sistemas de votación, crowdfunding, … y las aplicaciones del blockchain en otras áreas de la empresa distintas de la estrictamente financiera, como ya hemos visto, toman una realidad digna de considerar por parte del mundo empresarial.

6.2. VENTAJAS Y DESVENTAJAS EN LA ADOPCIÓN DE UNA CRIPTODIVISA DESCENTRALIZADA EN LA ACTIVIDAD DE LA EMPRESA, FRENTE AL DINERO FIAT O LOS MEDIOS DE PAGO TRADICIONALES

En el desarrollo del trabajo se han señalado una serie de ventajas relativas a la adopción de las criptodivisas y más en concreto del bitcoin, que se pueden resumir en las siguientes:

- Ausencia de intermediarios, o intermediarios con menores comisiones que en el caso de la moneda fiat, en un grado mayor o menor según el tipo de implementación elegido. Además, permite un ahorro de costes asociado al transporte seguro de la caja, … pese a que deba considerarse la seguridad de mantener un sistema propio.

- Eliminación de riesgos de corralitos, así como derivados de decisiones de carácter económico de gobiernos y entidades financieras.

- Relativo anonimato o privacidad en el uso. Mediante la correcta gestión de claves, asociadas a cuentas de bitcoin, se puede conseguir un alto grado de privacidad.

- Trazabilidad y transparencia de los pagos. El anonimato anterior se pierde por cabos sueltos estudiados bajo un ojo clínico como el de las autoridades de EEUU, que han resuelto casos gracias al carácter público del blockchain, como el del administrador de Silk Road sentenciado en 2015. También es posible en el caso de las empresas o incluso de los usuarios más avezados, de rastrear las actividades de los demás, si aquellos no son cuidadosos.

- Irreversibilidad de los pagos, esto dificulta algunos tipos de fraude, pero facilita otros, si bien está contemplado en el protocolo como condición de diseño.

- Existencia de un ecosistema ya desarrollado con unos agentes, en evolución, que ya han solucionado algunos problemas de diversa naturaleza y han ganado diversidad, reduciéndose su vulnerabilidad (nos referimos a los servicios alrededor de la moneda, la comunidad, …).

- Posibilidad de acceder a un mercado emergente, el de los usuarios de criptodivisas, que, atraídos por su filosofía, promesas y carácter innovador, buscan y paulatinamente van encontrando, más comercios donde utilizar el sistema en su vida diaria.

- Desarrollo de sinergias en la compañía, en caso de incorporarse un equipo especializado para la gestión de éstos activos, que podría facilitar el uso del blockchain integrado en otras áreas diferentes de la financiera, como la gestión de recursos humanos, de proyectos, ...

Por otro lado, también hemos comentado variadas desventajas que se pueden sintetizar en las que siguen:

- Algunas limitaciones técnicas a largo plazo comentadas en el apartado anterior, además de la irreversibilidad de pagos (y su riesgo ante errores del software o los usuarios), las precauciones a tener en cuenta en redes públicas que deberíamos contemplar en nuestro día a día pese a no usar criptodivisas, … o los peligros de ataques Sybil, DoS o de minado egoísta, podrían ser desventajas técnicas que en ocasiones también comparten los sistemas de pago convencionales.

- Tendencia a la volatilidad e influencia de la especulación (reducida en la práctica comercial por los procesadores de pagos o la especificación de políticas comerciales algo más detalladas), que hace recomendable ser prudente con su uso, especialmente, como almacén de valor.

- Desconfianza acerca de los motivos detrás de la creación del bitcoin y su mantenimiento, acerca de las posibles fuerzas que influyan en su existencia a nivel económico relacionadas con el riesgo de concentración geográfica, adopción de economías de escala y posibilidad de minado para atacar la moneda o favorecer intereses concretos, …

- Falta de regulación: la vulnerabilidad legal frente a pérdidas, robos o fraude de intermediarios del ecosistema bitcoin, la no obligatoriedad de información o aseguramiento por su parte, además del descuido de factores relativos a la posible cancelación de pagos, … perjudican el uso de las criptodivisas como medio de cambio de confianza.

Pese a que estos inconvenientes o riesgos son dignos de ser tenidos en cuenta, se ha de considerar racionalmente cómo afectan las probabilidades y los impactos que pueden tener a su carácter como riesgos. Los riesgos derivados de los aspectos técnicos, de la volatilidad y de la falta de regulación comentados, se ven reducidos de un modo prácticamente total si consideramos la inversión en un equipo técnico que mantenga un sistema propio de gestión y almacenamiento de bitcoins debidamente planificado y considerando la seguridad en las operaciones frente a todos los aspectos señalados.

La apuesta es igualmente posible para pequeñas empresas, si bien sería más interesante, en caso de no contar con la capacidad técnica suficiente, optar por intermediarios, vigilando su fiabilidad del modo que hemos comentado. El ecosistema bitcoin en particular, por su mayor recorrido, ha facilitado soluciones para todos y la confianza que podemos depositar en los intermediarios mejora paulatinamente, con ejemplos Coinbase, Coinffeine, … por los que han apostado bancos y entidades financieras.

Una vez sustraídos los tres factores mencionados, sólo nos queda la desconfianza como barrera. Esto depende de todos, dado que los fundamentos técnicos son lo suficientemente sólidos como para que el bitcoin sea una buena baza a largo plazo. Mientras se pueda reforzar su carácter descentralizado, la influencia de intereses particulares en su correcto funcionamiento como moneda se ve imposibilitada en una medida prácticamente total, si bien su aceptación y su distribución en términos geográficos, de mercado y de red, son clave para que esto suceda.

Siguiendo la línea de la empresa como usuario, cabe plantear la hipótesis del refuerzo que supondría en dicha descentralización, la introducción de empresas privadas, repartidas geográficamente y con diversidad de intereses, que generaría una suerte de competencia, más allá de su actividad propiamente dicha, para superarse en su posición como mineros dentro de la red y mantener un esquema que les permitiría mucho mayor control sobre su riqueza y les obligaría a mantenerse más alerta sobre su entorno.

Pese a lo ambicioso y favorable que sería un escenario como éste u otros que se nos podrían ocurrir, susceptibles de desarrollarse o planificarse a través de acuerdos privados o políticas institucionales, las ventajas reales y actuales son exclusivamente las que hemos señalado.

7. CONCLUSIONES

Gracias al esfuerzo realizado durante la elaboración de este trabajo, su autor se encuentra satisfecho al conocer los fundamentos del fenómeno de las criptodivisas y el blockchain y motivado a seguir su evolución en el futuro. Además, en éste apartado se resaltarán los aspectos que le han llamado especialmente la atención sobre el tema.

En primer lugar, es de subrayar cómo el concepto de blockchain, como base de datos distribuida en que se basan las criptomonedas, se trata de una tecnología sobre la que aún se están probando aplicaciones y variando pequeños detalles para conseguir un potencial que va mucho más allá de las presentes criptodivisas, con su naturaleza exclusivamente económica, como podemos ver reflejado en el apartado relativo a las aplicaciones del blockchain del segundo capítulo.

También es importante llamar la atención sobre la evolución de las criptomonedas desde la aparición del bitcoin, que pese haber reducido su capitalización relativa con la aparición de alternativas, aún mantiene una fuerza en el mercado mucho mayor que sus competidores, apareciendo constantemente nuevas opciones asociadas a ideas distintas de la original, que pretenden y probablemente terminen logrando, resolver muchos problemas asociados al esquema del bitcoin que hemos comentado, temas que se han desarrollado en los apartados relativos a la historia de las criptodivisas y el análisis que se ha hecho desde el punto de vista económico, en cuanto a los parámetros a tener en cuenta para la valoración de las distintas criptodivisas y la influencia de la tecnología detrás de las mismas en su evolución como criptomonedas.

Vinculado con esto, también se ha de destacar el carácter abierto de las criptodivisas y en especial del bitcoin, que permite poner en manos de sus usuarios la seguridad y privacidad de sus actividades económicas; y también el papel de la comunidad en que se apoyan, que da pie a mejoras, discutidas en foros de colaboradores y expertos, para resolver los nuevos retos que se van planteando.

Probablemente lo más llamativo de todo es cómo el conjunto de agentes implicados en el funcionamiento del ecosistema en torno a las criptodivisas, como exchanges, las propias comunidades de las criptodivisas, … son flexibles y se adaptan rápidamente a las nuevas problemáticas surgidas, proporcionando progresivamente más seguridad y alternativas en el mercado, según aumenta el tiempo que llevan en funcionamiento. Esta conclusión es resultado directo del análisis de dicho ecosistema desarrollado en el capítulo 4, en el que también se valora la cambiante regulación en cuanto a las criptodivisas y las actividades económicas vinculadas a ellas.

En lo relativo al uso por parte de empresas y la opinión de las principales entidades financieras, podemos observar que existe una preocupación por las ventajas inherentes al uso de criptodivisas descentralizadas que, aunque ponen en manos de los usuarios la seguridad de su dinero, con gran flexibilidad para adaptarse a las necesidades de los mismos en cada contexto de uso y menos costes de transacción, especialmente en cuanto operaciones internacionales, escapan al control de bancos y gobiernos con las consecuencias que esto puede tener. En el segundo apartado del capítulo 4 se comentan éstos aspectos y se enuncian diversas recomendaciones para que los comerciantes puedan operar en criptomonedas con un riesgo mínimo.

En el quinto capítulo se recogen las características y resultados de un estudio exploratorio a través de entrevistas estructuradas breves del que el autor ha conseguido extraer ciertas conclusiones útiles. Una de ellas es la existencia entre 2012 y 2014, de un periodo en el que el bitcoin fue una novedad tecnológica en boga que algunas empresas trataron de aprovechar para su propia publicidad, pero renunciaron posteriormente a su uso por considerar que ya no era interesante desde el

punto de vista comercial. También llama la atención las veces que es destacada en las respuestas, su ventaja frente a otros medios tradicionales para empresas que operan a nivel internacional, en comparación con otros negocios de proyección geográfica más concreta que parecen tener menor público interesado en dicha forma de pago. En cuanto a la forma de aceptar los pagos, destaca el uso de procesadores de pagos con bitcoin, aunque también se suelan utilizar wallets propias de forma paralela. De todos modos, estas conclusiones podrían ser contrastadas con un estudio más profundo, como se explica en el capítulo siguiente sobre propuestas de mejora. Relacionado con esto, se ha intentado también consultar sin éxito a la Oficina Nacional de Investigación del Fraude (ONIF), a sugerencia de uno de los entrevistados, dado que aquella ha realizado investigaciones con el objetivo de conocer la regularidad fiscal y la operativa en las transacciones con bitcoin, de diversas empresas que lo utilizan.

El trabajo concluye con una comparación de las tecnologías preponderantes en el mundo de las criptodivisas y un resumen de ventajas e inconvenientes de las mismas frente a la moneda fiat, destacando como desventajas la volatilidad y regulación insuficiente y cambiante, además de algunos problemas técnicos que aún afectan a la red.

8. PROPUESTAS DE MEJORA

Tomando como referencia el trabajo elaborado, se pretende, en éste capítulo, identificar algunos de las posibles líneas de ampliación y mejora del mismo, siendo las más importantes, las siguientes:

- Realizar un análisis en profundidad con una muestra representativa, de tipo descriptivo, evaluando variables como el ahorro de los negocios por la aplicación del bitcoin en las operaciones como medio de pago, las opciones y motivos por los que las empresas lo aceptan, …

- Realizar un estudio de viabilidad acerca de las actividades de minado en el momento actual, atendiendo a las distintas modalidades existentes.

- Estudiar con más detalle la regulación de aplicación en materia fiscal y mercantil para llevar a cabo actividades de casa de cambio de criptodivisa, minería, … o simplemente para operar en bitcoin u otras criptodivisas.

- Analizar más en profundidad el funcionamiento específico de algunos de los nuevos agentes como procesadores de pago y exchanges, surgidos en torno a las criptodivisas.

- Proponer un plan de uso concreto de la tecnología enunciada, para casos en los que la eficiencia en costes podría ser especialmente interesante, como la operación en países diversos con distintas monedas de una empresa, que podría reducir los costes relativos a las transacciones internacionales utilizando alguna forma de criptomoneda o el uso de aplicaciones basadas en el blockchain como los Smart Contracts.

9. ANEJO I: FORMATOS DE ENCUESTA

9.1. FORMATO EN ESPAÑOL 1:

¿Cuál era su objetivo al aceptar bitcoin?

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

> ¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

> ¿Qué ahorro obtiene por cada compra?
>
> ¿Número e ingreso de ventas en bitcoin de uno o varios artículos?
>
> ¿Número e ingreso de ventas en otros métodos de los mismos artículos?

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

¿Desde cuándo acepta bitcoin?

9.2. FORMATO EN ESPAÑOL 2:

¿Cuál era su objetivo al aceptar bitcoin?

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

> ¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

> ¿Qué ahorro obtiene por cada compra?
>
> ¿Beneficio obtenido de algún artículo individual pagado en bitcoin?
>
> ¿Beneficio obtenido de dicho artículo, adquirido con otros medios de pago?

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

¿Desde cuándo acepta bitcoin?

9.3. FORMATO EN INGLÉS 1:

What goals do you try to achieve by accepting bitcoin?

Do you get clients for they are especially interested in using this payment option?

How many people pay in bitcoins each week/month/year?

Do you save any costs by getting bitcoins instead of cash or plastic money?

How much money do you save each purchase?

Could you tell me the number of sales and profit you made from products which were purchased in bitcoins?

Could you tell me the same information of the previous products when they were paid using other payment options?

What kind of method do you use to get bitcoin payments? Do you use bitcoin payment processors such as Coinbase? or Do you have your own system to store the bitcoins you get?

Do you pay in bitcoins to your suppliers? If you do, Do you save any money for it?

Since when do you accept bitcoin as a payment option?

9.4. FORMATO EN INGLÉS 2:

Why do you accept bitcoin?

Do you get clients for they are especially interested in using this payment option?

How many people pay in bitcoins each week/month/year?

Do you save any costs by getting bitcoins instead of cash or plastic money?

How much money do you save each purchase?

Could you tell me the profit you made from a sale which was paid in bitcoin?

Could you tell me the profit you made from a sale of the same product which was paid by other payment options?

What kind of method do you use to get bitcoin payments? Do you use bitcoin payment processors such as Coinbase? or Do you have your own system to store the bitcoins you get?

Do you pay in bitcoins to your suppliers? If you do, Do you get any advantage from doing it?

Since when do you accept bitcoin as a payment option?

10. ANEJO II: RESPUESTAS

10.1. ABANLEX

¿Cuál era su objetivo al aceptar bitcoin?

- *[Co-fundador, Fernández P.] Investigar e innovar*

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

- *[Co-fundador, Fernández P.] No*

¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

- *[Co-fundador, Fernández P.] 0/año*

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

- *[Co-fundador, Fernández P.] No*

¿Qué ahorro obtiene por cada compra?

- *[Co-fundador, Fernández P.] 0*

¿Número e ingreso de ventas en bitcoin de uno o varios artículos?

- *[Co-fundador, Fernández P.] 0*

¿Número e ingreso de ventas en otros métodos de los mismos artículos?

- *[Co-fundador, Fernández P.] 0*

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

- *[Co-fundador, Fernández P.] Bitpay y transferencia simple*

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

- *[Co-fundador, Fernández P.] No*

¿Desde cuándo acepta bitcoin?

- *[Co-fundador, Fernández P.] 2013*

10.2. HOTEL NABIA

- *[Directores, O'Shea I. y Bernar S.] El motivo de aceptar bitcoins fue puramente MARKETING, ser el primer hotel en algo es siempre bueno y aparecimos en muchos medios por eso.*

Empezamos a aceptar bitcoins en 2013, UNA SOLA persona ha utilizado bitcoins como medio de pago en 3 años, el importe no llegó a 300 euros.

Ya no aceptamos bitcoins, el momento de la novedad y la ventaja del marketing ha pasado.

10.3. TU TÓNER BARATO

¿Cuál era su objetivo al aceptar bitcoin?

- *[Atención al cliente] Captar clientes*

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

- *[Atención al cliente] No, solo un pago en 2 años que estuvo activo*

¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

- *[Atención al cliente] 1 pedido en 2 años*

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

- *[Atención al cliente] Peores que la tarjeta, pero mejores que paypal o contra reembolso*

¿Qué ahorro obtiene por cada compra?

- *[Atención al cliente] Alrededor de un 1%*

¿Número e ingreso de ventas en bitcoin de uno o varios artículos?

- *[Atención al cliente] No llego a los 100 euros el único pedido*

¿Número e ingreso de ventas en otros métodos de los mismos artículos?

- *[Atención al cliente] Más de 5000€ euros al mes.*

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

- *[Atención al cliente] Procesadores de pagos*

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

- *[Atención al cliente] No, ni por asomo me aceptarían dicha forma de pago*

¿Desde cuándo acepta bitcoin?

- *[Atención al cliente] Ya no lo aceptamos, pero lo hicimos de 2013 a 2016.*

10.4. DDHH

- *[CEO, Fernández D.] Aceptamos y usamos bitcoin por una cuestión ideológica, dado que a nivel comercial nos parece un poco prematuro plantearse el uso de bitcoin ahora mismo. No obstante, han sido varios los clientes que se han interesado en nosotros precisamente por aceptar bitcoin. Entendemos que, para operaciones comerciales internacionales, Bitcoin es mucho más eficiente en tanto que no existen gastos derivados del cambio de moneda, de cambio de banco, fronteras, etc.… además de que el pago es inmediato, y no se ha de esperar 4 o 5 días cuando es un cliente de, por ejemplo, Japón, el que nos paga.*

  Aun así, nuestro mejor cliente nos llegó porque buscaban un despacho que admitiese bitcoin como forma de pago. Y claro, cuando eres casi el único que ofrece una solución adicional de pago, pues tienes muchas papeletas de que ese tipo de cliente te contrate. Es el momento de aceptar bitcoin, sin duda.

  Es una bienvenida a todo aquello que agilice y dinamice la tecnología y con ello una nueva forma de concebir internet y la forma de comunicarnos las personas. Una forma descentralizada y por tanto más libre.

10.5. BUCARELLI

- *[Atención al cliente] Nunca he vendido nada por bitcoin. No tengo desde hace 2 años.*

10.6. JJGAMES.COM

Why do you accept bitcoin?

- *[Founder, Hendricks J.J.] I like using bitcoin myself and storing some money in bitcoin. When I heard about it I thought it would be good to offer it for people buying on our site too.*

Do you get clients for they are especially interested in using this payment option?

- *[Founder, Hendricks J.J.] Yes. We get people coming to the site specifically because we offer bitcoin.*

How many people pay in bitcoins each week/month/year?

- *[Founder, Hendricks J.J.] It isn't very big, but we are a fairly small retailer too. We get 1 payment a week on average.*

Do you save any costs by getting bitcoins instead of cash or plastic money?

- *[Founder, Hendricks J.J.] Yes. We save about 3.5% on payment processing fees because we don't have to pay credit card companies.*

How much money do you save for each purchase?

- *[Founder, Hendricks J.J.] See above.*

Could you tell me the profit you made from some sale which was paid in bitcoin?

- *[Founder, Hendricks J.J.] Not sure what you mean. On average we save about $0.90 on each transaction so we make an additional $0.90 from selling with bitcoin.*

Could you tell me the profit you made from a sale of the same product which was paid by other payment options?

What kind of method do you use to get bitcoin payments? Do you use bitcoin payment processors such as Coinbase? or Do you have your own system to store the bitcoins you get?

- *[Founder, Hendricks J.J.] We use BitPay now for our bitcoin payments. We used to do it ourselves, but it was too prone to errors so we decided to process through someone else who specializes in this.*

¿Do you pay in bitcoins to your suppliers? If you do, Do you get any advantage from doing it?

- *[Founder, Hendricks J.J.] Nope.*

Since when do you accept bitcoin as a payment option?

- *[Founder, Hendricks J.J.] Since 2010 if I remember correctly. My lead programmer was an early adopter and he helped convince me to adopt it too.*

10.7. BITCOIN INVESTORS OF TRUST

¿Cuál era su objetivo al aceptar bitcoin?

- *[CEO, Pavón M. J.] Cambiar el sistema económico actual.*

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

- *[CEO, Pavón M. J.] Sí claro.*

¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

- *[CEO, Pavón M. J.] Ahora unos 50.*

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

- *[CEO, Pavón M. J.] Sí claro.*

¿Qué ahorro obtiene por cada compra?

- *[CEO, Pavón M. J.] 5% aproximadamente*

¿Beneficio obtenido de algún artículo individual pagado en bitcoin?

- *[CEO, Pavón M. J.] Mayor que con el pago en fiat.*

¿Beneficio obtenido de dicho artículo, adquirido con otros medios de pago?

- *[CEO, Pavón M. J.] Menor que con bitcoin.*

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

- *[CEO, Pavón M. J.] BTCfacil.*

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

- *[CEO, Pavón M. J.] Sí claro.*

¿Desde cuándo acepta bitcoin?

- *[CEO, Pavón M. J.] 2013.*

10.8. UNIÓN EDITORIAL

- *[Director, Marcos J. P.] Actualmente ya no recibimos ningún pago por Bitcoin hace dos años cuando terminó la moda de los bitcoin.*

10.9. DEPORTES PINEDA

- *[Gómez P.] Lamentablemente en esta tienda se lleva aceptando bitcoin desde el 2012 pero no ha habido ninguna compra con ellos.*

10.10. THE GEOGRAPHIC CLUB

¿Cuál era su objetivo al aceptar bitcoin?

- *[Atención al cliente] Me lo pidió un conocido*

¿Recibe mayor público porque dicho público esté interesado en utilizar este medio de pago?

- *[Atención al cliente] No*

¿Cuántos individuos/pedidos a la semana/mes/año recibe que pagan con bitcoin?

- *[Atención al cliente] 5 al mes*

¿Consigue menores costes de transacción/mayores beneficios en la práctica que con los pagos por transferencia/efectivo/tarjeta?

- *[Atención al cliente] No*

¿Qué ahorro obtiene por cada compra?

- *[Atención al cliente] Nada*

¿Beneficio obtenido de algún artículo individual pagado en bitcoin?

- *[Atención al cliente] Ninguno*

¿Beneficio obtenido de dicho artículo, adquirido con otros medios de pago?

- *[Atención al cliente] Ninguno*

¿Qué solución utiliza? ¿Utiliza procesadores de pago u opera directamente en bitcoins?

- *[Atención al cliente] Directamente bitcoins*

¿Opera en bitcoin con sus proveedores? ¿Si es así lo hace por ahorros en costes?

- *[Atención al cliente] No*

¿Desde cuándo acepta bitcoin?

- *[Atención al cliente] Desde hace 1 año y medio*

10.11. TEALET

Why do you accept bitcoin?

- *[Founder, Petersen E.] It is a more efficient way for us to accept payment across borders and currencies.*

Do you get clients for they are especially interested in using this payment option?

- *[Founder, Petersen E.] Sometimes bitcoin users want to support businesses that accept bitcoin, but mostly people use it when it is more efficient. An example of this is when a customer from a foreign country can pay with bitcoin instead of having to pay a fee to exchange their currency to USD for the credit card transaction.*

How many people pay in bitcoins each week/month/year?

- *[Founder, Petersen E.] We get about two bitcoin payment transactions per month.*

Do you save any costs by getting bitcoins instead of cash or plastic money?

- *[Founder, Petersen E.] Yes, we save about 3% versus using credit card to accept payments.*

How much money do you save each purchase?

- *[Founder, Petersen E.] 3%*

Could you tell me the profit you made from some sale which was paid in bitcoin?

- *[Founder, Petersen E.] I don't think I understand your question. We immediately exchange the bitcoin to USD when we receive the payment so there is no profit or loss.*

Could you tell me the profit you made from a sale of the same product which was paid by other payment options?

- *[Founder, Petersen E.] No difference from accepting cash. We actually offer a 3% discount for bitcoin payments on our website because we would have to pay that 3% if we accepted credit card.*

What kind of method do you use to get bitcoin payments? Do you use bitcoin payment processors such as Coinbase? or Do you have your own system to store the bitcoins you get?

- *[Founder, Petersen E.] We use Coinbase. We built our own payment processor for litecoin payments.*

Do you pay in bitcoins to your suppliers? If you do, Do you get any advantage from doing it?

- *[Founder, Petersen E.] We use Bitcoin through payments with Align Commerce. The funds reach the supplier in their local currency though, so they never see the bitcoin.*

Since when do you accept bitcoin as a payment option?

- *[Founder, Petersen E.] We started to accept bitcoin in September 2013.*

11. BIBLIOGRAFÍA

Accenture. 2015. *Blockchain in the Investment Bank*. En: Accenture [en línea]. [Consulta: 31 Marzo 2016]. Archivo pdf. Disponible en: https://www.accenture.com/t20150811T015521__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-Blockchain-Investment-Bank.pdf

Bitfury Group. 2015. *Proof of Stake versus Proof of Work*. En: bitfury.com [en línea]. [Consulta: 19 Abril 2016]. Archivo pdf. Disponible en: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf

Chaum, D. 1983. Blind Signatures for Untraceable Payments. En: RIVEST, R. L.; SHERMAN, A. T.; CHAUM D. *Advances in Cryptology* [en línea]. California: Prooceedings of Crypto 82, Session III, p. 199-203. [Consulta: 15 Febrero 2016]. Versión pdf. Disponible en DOI: 10.1007/978-1-4757-0602-4_18. Disponible en: http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

Consumer Financial Protection Bureau (CFPB) 2014. *Risks to consumers posed by virtual currencies.* En: CFPB [sitio web]. EEUU: Consumer Financial Protection Bureau. [Consulta: 1 Abril 2016]. Disponible en: http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf

Deloitte. 2015. *State-Sponsored Cryptocurrency: Adapting the best of Bitcoin's Innovation to the Payments Ecosystem*. En: Deloitte [en línea]. Estados Unidos: Deloitte. [Consulta: 31 Marzo 2016]. Archivo pdf. Disponible en: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-state-sponsored-cryptocurrency.pdf

EBA Working Group on electronic and alternative payments. 2015. *Cryptotechnologies, a major IT innovation and catalyst for change.* En: EBA [sitio web]. Unión Europea: European Banking Authoriry. [Consulta: 1 Abril 2016]. Disponible en: https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf

European Banking Authority (EBA). 2014. *EBA Opinion on 'virtual currencies'.* En: EBA [sitio web]. Unión Europea: European Banking Authoriry. [Consulta: 1 Abril 2016]. Disponible en: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

España. 2015. Proposición no de ley 162/001128 del 7 de Enero de 2015 por Díez González Rosa María. *Boletín Oficial de las Cortes Generales*, 7 de Enero de 2015, Serie D, Núm.592, página 16-17 [Consulta: 3 Mayo 2016].

España. 2014. Pregunta escrita al congreso 184/47663, 3 de Marzo de 2014 por Anchuelo Greco Álvaro. *Congreso de los Diputados, Secretaría General, Registro General*, 8 de Mayo de 2014, entrada 134379 [Consulta: 3 Mayo 2016].

Europa. 2015. Sentencia del Tribunal de Justicia de la Unión Europea (TJCE) (sala quinta) TJCE\2015\244, 22 de Octubre de 2015. Thomson Reuters Aranzadi. [Consulta: 3 Mayo 2016].

Farell, R. 2015. An Analysis of the Cryptocurrency Industry. En: *Wharton Research Scholars Journal*, Paper 130 [en línea]. [Consulta: 09 Marzo 2016]. Archivo pdf. Disponible en: http://repository.upenn.edu/cgi/viewcontent.cgi?article=1133&context=wharton_research_scholars

Financial Action Task Force (FATF). 2014. *Virtual Currencies - Key Definitions and Potential AML/CFT Risks*. En: FATF [en línea]. Estados Unidos: FATF/OECD. [Consulta: 15 Febrero 2016]. Archivo pdf. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Crimes Enforcement Network (FinCEN). 2013. *Guidance. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. En: FinCEN [en línea]. Estados Unidos: FinCEN. [Consulta: 15 Febrero 2016]. Archivo pdf. Disponible en: https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

Houy, N. 2014. *It will cost you nothing to "kill" a Proof-of-Stake crypto-currency.* En: HAL-SHS (Sciences de l'Homme et de la Société) [en línea]. Francia: Groupe D'Analyse et de Théorie Économique Lyon-St Étienne. [Consulta: 6 Abril 2016]. Archivo pdf. Disponible en: https://halshs.archives-ouvertes.fr/halshs-00945053/document

King, S.; Nadal, S. 2012. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. En: peercoin.org [en línea]. [Consulta: 6 Abril 2016]. Archivo pdf. Disponible en: https://peercoin.net/assets/paper/peercoin-paper.pdf

Lo S., Wang J. C. 2014. *Bitcoin as Money?.* En: www.bostonfed.org [En línea]. [Consulta: 21 Junio 2016]. Archivo pdf. Disponible en: https://www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1404.pdf

Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. 2016**.** *Bitcoin and Cryptocurrency Technologies.* Borrador. EEUU: Princeton University Press. [Consulta: 20 Abril 2016]. Archivo pdf. Disponible en: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. En: bitcoin.org [en línea]. [Consulta: 6 Abril 2016]. Archivo pdf. Disponible en: https://bitcoin.org/bitcoin.pdf

Schwartz, D.; Youngs, N. y Britto, A. 2014. *The Ripple Protocol Consensus Algorithm.* En: Ripple Labs Inc. [en línea]. [Consulta: 6 Abril 2016]. Archivo pdf. Disponible en: https://ripple.com/files/ripple_consensus_whitepaper.pdf

The Clearing House. 2014. *Virtual currency risks and regulation*. En: The Clearing House [en línea]. Estados Unidos: The Clearing House. [Consulta: 29 Marzo 2016]. Archivo pdf. Disponible en: https://www.theclearinghouse.org/~/media/Files/Research/20140623_Virtual_Currency White Paper.pdf

Yingjie, Z. 2015. Cryptocurrency brings new battles into the currency market. En: GEORG CARLE, DANIEL RAUMER y LUKAS SCHWAIGHOFER (eds.). *Proceedings of the Seminars Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM), Winter Semester 2014/2015,* volumen NET-2015-03-1 de *Network Architectures and Services (NET).* Munich (Germany): Marzo 2015. Chair for

Network Architectures and Services, Department of Computer Science, Technische Universität München, pp. 91-99. [Consulta: 9 Marzo 2016]. Archivo pdf. Disponible en: http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-03-1/NET-2015-03-1_13.pdf

12. WEBGRAFÍA

Biggs, J. 2015. *Ascribe Raises $2 Million To Ensure You Get Credit For Your Art.* En: techcrunch.com. [Sitio web]. 24 Jun. 2015 [Consulta: 17 Junio 2016]. Disponible en: https://techcrunch.com/2015/06/24/ascribe-raises-2-million-to-ensure-you-get-credit-for-your-art

bitcoin.org. 2016. [sitio web]. [Consulta: 30 Marzo 2016]. Disponible en: https://bitcoin.org

bitcoincharts.com. 2016. [sitio web]. [Consulta: 18 Abril 2016]. Disponible en: http://bitcoincharts.com/charts/volumepie/

Bitpay. 2016. [sitio web]. [Consulta: 30 Marzo 2016]. Disponible en: https://bitpay.com/pricing

blockchain.info 2016. *Distribución de tasas de hash: Una estimación de la distribución de las tasas de hash entre los pools de minería de mayor tamaño* [sitio web]. [Consulta: 25 Marzo 2016]. Disponible actualizado en: https://blockchain.info/pools?timespan=24hrs

Boneh, D. 2015. *Message Integrity*. *Cryptography I.* En: Cousera [sitio web]. EEUU: Stanford University. [Consulta: 20 Abril 2016]. Disponible en: https://www.coursera.org/learn/crypto/

Boulton, C. 2015. *BNY Mellon Explores Bitcoin's Potential*. En: The Wall Street Journal [blog]. 5 Abr. 2015 [Consulta: 1 Abril 2016]. Disponible: http://blogs.wsj.com/cio/2015/04/05/bny-mellon-explores-bitcoins-potential/

Coinbase. 2016. [sitio web]. [Consulta: 30 Marzo 2016]. Disponible en: https://www.coinbase.com/merchants

Coindesk. 2015. *How to Store Your Bitcoins.* En: www.coindesk.com [sitio web]. [Consulta: 30 Marzo 2016]. Disponible en: http://www.coindesk.com/information/how-to-store-your-bitcoins/

Coinmarketcap. 2016. *Crypto-Currency Market Capitalizations* [sitio web]. [Consulta: 25 Mayo 2016]. Disponible en: http://coinmarketcap.com

Dermot, M. 2007. *Digital Cash. Network Security lecture notes*. En: Birmingham University [sitio web]. Reino Unido: Birmingham University. [Consulta: 15 Febrero 2016]. Disponible en: https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html

Higginbotham, S. 2015. *This startup raised $5 million to bring the blockchain to the Internet of things.* En: fortune.com. [sitio web]. 18 Ag. 2015. [Consulta: 17 Junio 2016]. Disponible en: http://fortune.com/2015/08/18/filament-blockchain-iot

King R. 2015. *UBS Working with Blockchain Prototypes*. En: The Wall Street Journal [blog]. 2 Oct. 2015 [Consulta: 1 Abril 2016]. Disponible: http://blogs.wsj.com/cio/2015/10/02/ubs-working-with-blockchain-prototypes/

Lacey, S. 2016. *The Energy Blockchain: How Bitcoin Could Be a Catalyst for the Distributed Grid.* En: greentechmedia.com. [Sitio web]. 26 Feb. 2016 [Consulta: 17 Junio 2016]. Disponible en: http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid

Library of Congress. 2015. *Regulation of Bitcoin in Selected Jurisdictions* [sitio web]. [Consulta: 25 Marzo 2016]. Disponible en: http://www.loc.gov/law/help/bitcoin-survey/

Lombardo, H. 2015. *Hollywood Cloud Firm Developing Blockchain-Based IP Protection System for Entertainment Content*. En: allcoinsnews.com. [Sitio web]. 30 Jul. 2015 [Consulta: 17 Junio 2016]. Disponible en: http://allcoinsnews.com/2015/07/30/hollywood-cloud-firm-developing-blockchain-based-ip-protection-system-for-entertainment-content

Long M. 2015. *Ripple Adds Santander InnoVentures Fund as Series A Investor*. En: Ripple [sitio web]. [Consulta: 1 Abril 2016]. Disponible: https://ripple.com/ripple_press/ripple-adds-santander-innoventures-fund-as-series-a-investor/

McMillan, R. 2014. *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*. En: Wired [sitio web]. [Consulta: 30 Marzo 2016]. Disponible en: http://www.wired.com/2014/03/bitcoin-exchange/

Otto C. 2015. *Del ninguneo al miedo: la banca española espabila para que internet no le 'robe' negocio.* En: El Confidencial [sitio web]. [Consulta: 20 Abril 2016]. Disponible: http://www.elconfidencial.com/tecnologia/2015-09-21/del-ninguneo-al-miedo-asi-se-esta-moviendo-la-banca-espanola-para-que-internet-no-le-quite-negocio_1019969/

Payeras, M; Isern, A. P.; Mut, M. 2014. *Sistemas de pago electrónico*. En: CryptoRed, Universidad Politécnica de Madrid [sitio web]. [Consulta: 24 Marzo 2016]. Disponible en: http://www.criptored.upm.es/crypt4you/temas/sistemaspago/leccion3/leccion03.html

Rizzo, P. 2015. *Satoshi Nakamoto 'Unmasking' Might Be Driving Bitcoin's Price Rally.* En: www.coindesk.com [sitio web]. [Consulta: 25 Marzo 2016]. Disponible en: http://www.coindesk.com/satoshi-nakamoto-unmasking-might-be-driving-bitcoins-price-rally/

Rizzo, P. 2015. *Why Microsoft Wants 'Every Blockchain' on its Azure Platform.* En: www.coindesk.com [sitio web]. [Consulta: 1 Abril 2016]. Disponible en: http://www.coindesk.com/microsoft-blockchain-azure-marley-gray/

Simonite, T. 2015. *Los bancos copian la tecnología Bitcoin para adaptarla a sus necesidades.* En: MIT Technology Review [sitio web]. [Consulta: 1 Abril 2016]. Disponible en: http://www.technologyreview.es/informatica/48275/los-bancos-copian-la-tecnologia-bitcoin-para/

Simonite, T. 2015. *La gran apuesta de Microsoft para las transacciones del futuro se inspira en Bitcoin.* En: MIT Technology Review [sitio web]. [Consulta: 1 Abril 2016]. Disponible en: https://www.technologyreview.es/informatica/49102/la-gran-apuesta-de-microsoft-para-las/

Simonite, T. 2015. *Ripple Labs fabrica dinero.* En: MIT Technology Review [sitio web]. [Consulta: 1 Abril 2016]. Disponible en: http://www.technologyreview.es/informatica/44847/puesto-50-ripple-labs-fabrica-dinero/

Suberg, W. 2015. *Factom's Latest Partnership Takes on US Healthcare.* En: cointelegraph.com. [sitio web]. 23 Abr 2015 [Consulta: 17 Junio 2016]. Disponible en: http://cointelegraph.com/news/factoms-latest-partnership-takes-on-us-healthcare