FACULTAD DE TURISMO Y FINANZAS

GRADO EN FINANZAS Y CONTABILIDAD

EL BITCOIN: ANÁLISIS Y EVOLUCIÓN

Trabajo Fin de Grado presentado por Francisco Alonso Fernández, siendo la tutora del mismo la profesora Rosario Gómez-Álvarez Díaz.

Vº. Bº. de la Tutora: Alumno/a:

Dª. Rosario Gómez-Álvarez Díaz D. Francisco Luis Alonso Fernández

Sevilla. Noviembre de 2017

GRADO EN FINANZAS Y CONTABILIDAD

FACULTAD DE TURISMO Y FINANZAS

TRABAJO FIN DE GRADO

CURSO ACADÉMICO [2017-2018]

TÍTULO:

EL BITCOIN: ANÁLISIS Y EVOLUCIÓN

AUTOR:

D. FRANCISCO LUIS ALONSO FERNÁNDEZ

TUTORA:

Dª. ROSARIO GÓMEZ-ÁLVAREZ DÍAZ

DEPARTAMENTO:

ECONOMÍA E HISTORIA ECONÓMICA

ÁREA DE CONOCIMIENTO:

ECONOMÍA APLICADA

RESUMEN:

Mediante la elaboración de este trabajo se ha querido dar una visión general y sencilla de los elementos claves para conocer que es el bitcoin, como funciona y su evolución. Por ello presentamos los elementos técnicos básicos de su funcionamiento: la criptografía y el blockchain, que son básicos para entender las cuestiones relacionadas con su implantación, seguridad y estabilidad. Asimismo recogemos el perfil actual del usuario, su evolución en el tiempo y la presencia en diferentes países. Por último, se analizan las ventajas, inconvenientes y perspectiva del futuro. Finalizamos con una serie de conclusiones.

PALABRAS CLAVE:

Bitcoin; Criptodivisa; Blockchain; Satoshi Nakamoto; Mining pools.

ÍNDICE

CAPÍTULO 1

INTRODUCCIÓN

1.1. INTRODUCCIÓN

Nos encontramos en un mundo donde la ciencia evoluciona y con ella, las tecnologías, que en muchos casos persigue la mejora del bienestar de las personas. Un claro ejemplo de ello se puede ver en las prestaciones de servicios que cada vez resultan más cómodas para las personas.

Uno de los temas con mayor importancia en la actualidad, son las diferentes formas de pago, ya que las transferencias por internet han aumentado y la gente intenta buscar la manera más fácil y económica para realizarlas. Por esta misma razón, en los últimos años se ha producido el surgimiento de una nueva moneda que está revolucionando el sistema virtual, el Bitcoin, una criptodivisa o moneda electrónica, también conocida por sus siglas BTC.

Esta moneda tiene su origen durante la crisis económica y financiera del año 2008, donde el entramado financiero se vino abajo, contemplando muchos clientes de las sociedades bancarias y financieras cómo sus ahorros, sus inversiones... se desplomaban sin poder hacer nada. El hecho de que el bitcoin no dependa de ninguna autoridad central que lo controle o gestione ha propiciado su expansión.

A día de hoy la utilización de las monedas oficiales son la base de los sistemas monetarios y de las transacciones económicas. Sin embargo, el empleo del Bitcoin se encuentra en auge; es innegable, tras superar la cotización del oro. Cada vez aparece con más frecuencia en los periódicos, en las noticias, tiene un mayor impacto su cotización, la banca tradicional y las autoridades se interesan por saber cómo funciona.

Por ello el presente trabajo pretende explicar los principales elementos que intervienen en el funcionamiento de esta moneda y su evolución desde su aparición en 2008 hasta mediados de 2017.

Tras esta introducción, el capítulo 2 se centra en la definición, el origen y la explicación de sus dos fundamentos tecnológicos: la criptografía y el blockchain. En el capítulo 3 se describe los componentes principales del bitcoin y su funcionamiento como sistema. El capítulo 4 se centra en el uso del bitcoin: perfil de usuarios, su evolución en el tiempo y la presencia en diferentes países. En el siguiente capítulo se analizan las ventajas, inconvenientes y perspectiva del futuro. Finalizamos con una serie de conclusiones.

CAPÍTULO 2

EL BITCOIN

2.1. ¿QUÉ ES BITCOIN? DEFINICIÓN Y ORIGEN

Bitcoin es un medio de pago mediante internet, y por lo cual, se considera una moneda virtual que usa algoritmos criptográficos, un protocolo y un software. La conjunción de estos componentes permite la realización de transacciones casi instantáneas entre pares (peer-to-peer o P2P, o red de "pares") y, por consiguiente, pagos en todo el mundo con unos costes de procesado de dichas transacciones muy reducidos, o incluso nulos.

La primera aparición pública de Bitcoin se produjo en la lista de criptografía de metzdowd[1], donde un usuario con el pseudónimo «Satoshi Nakamoto» anunció, el 1 de noviembre de 2008, que había estado trabajando en un nuevo sistema de dinero electrónico, resumiendo sus propiedades y el contenido del artículo original que describía su trabajo y que se encontraba disponible en el portal de Bitcoins[2]. A continuación presentamos el resumen que ofrecía su autor (Nakamoto, 2008):

"He estado trabajando en un nuevo sistema de pago electrónico que es totalmente peer-to-peer, sin una tercera parte que sirva de garante"

Las principales propiedades son:

- La falsificación se evita con una red peer-to-peer.
- No hay una tercera parte garante.
- Los participantes pueden ser anónimos.
- Las nuevas monedas se crean mediante un sistema denominado "prueba-del-trabajo".
- La "prueba de trabajo" para la creación de nuevas monedas también potencia la red para evitar la falsificación de la moneda.

El 11 de febrero de 2009, un perfil creado en el portal P2P foundation, también con el nombre de «Satoshi Nakamoto», publicó un mensaje: "Bitcoin open source implementation of P2P currency"[3]. En el texto, «Satoshi» daba a conocer el portal oficial de Bitcoin, las características fundamentales de éste, el artículo donde se describía el diseño e, incluso, el cliente inicial con el que comenzar a participar en la red.

Por el momento la identidad del creador, o creadores, no ha sido revelada. «Satoshi Nakamoto» es el pseudónimo que fue utilizado por la persona, o el grupo de personas que diseñaron y crearon la red Bitcoin, con el fin de mantener el anonimato y así protegerse a ellos mismos y a la red.

Lo único que se sabe de «Satoshi Nakamoto» son los datos publicados en su perfil del portal P2Pfoundation: hombre de nacionalidad japonesa y 38 años de edad (en el momento de publicación de este documento). Sin embargo, no es posible demostrar

[1] Consultado el 19/06/2017 en http://www.metzdowd.com/mailman/listinfo/cryptography

[2] Consultado el 19/06/2017 en http://www.bitcoin.org

[3] Consultado el 25/06/2017 en http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

que estos datos sean reales. Además, dado el diseño de Bitcoin, se le pueden atribuir conocimientos avanzados en criptografía y algoritmos matemáticos.

Hay muchas especulaciones sobre la identidad real que se esconde detrás de este pseudónimo. Una de ellas apuntaría a que se trata de Shinichi Mochizuki, matemático especializado en teoría de números y profesor de la Universidad de Kioto. Otras especulaciones enlazan la figura de «Nakamoto» con identidades relacionadas con mercados negros y negocios criminales.

2.2. FUNDAMENTOS DEL BITCOIN: LA CRIPTOGRAFÍA Y EL BLOCKCHAIN

El Bitcoin funciona como un libro contable, donde la información se registra en una serie de direcciones públicas en internet, similar a una cuenta corriente, donde el número de esa cuenta lo puede conocer cualquiera. Si el dueño de la cuenta realiza un pago, se registra en esa cuenta un debe, y por tanto debe existir otra cuenta de otra persona donde se registrará un haber. Pues bien, ese proceso, tal y como explica Rosembuj (2015), se fundamenta en dos elementos: la seguridad generada mediante métodos criptográficos, y un sistema descentralizado de confirmación de las transacciones, denominado blockchain. Por ello, consideramos necesarios explicar estos dos elementos para comprender el funcionamiento del bitcoin.

2.2.1. La criptografía

La criptografía como explica Rosembuj (2015), es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados. Es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. En origen, su único objetivo era el proteger la confidencialidad de informaciones militares y políticas. Sin embargo, en la actualidad es una ciencia interesante no sólo en esos campos, sino para cualquier otro que esté interesado en la confidencialidad de unos determinados datos.

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. El objetivo es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto el tipo de propiedades de las que se ocupa la criptografía son:

- Confidencialidad. Consiste en garantizar que sólo las personas autorizadas tienen acceso a la información. Para conseguirlo se utiliza códigos y técnicas de cifrado.

- Integridad. Garantiza la corrección y completitud de la información, es decir, el mensaje que leemos es el mismo que nos enviaron. Para conseguirlo puede usarse por ejemplo funciones hash criptográficas MDC.

- Autenticación. Proporciona mecanismos que permiten verificar la identidad del comunicador. El emisor del mensaje es quien dice ser, y no otro. Para conseguirlo se puede emplear por ejemplo función hash criptográfica MAC

Según la web “wikipedia.org”[4], un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.

Dentro del sistema bitcoin hay tres aspectos importantes de la criptografía:

[4] Consultado el 26/06/2017 en https://es.wikipedia.org/wiki/Criptograf%C3%ADa

1. Cifrado y decodificación

    - Algoritmos enfocados en convertir el texto plano en texto cifrado y viceversa, usado principalmente para asegurar su confidencialidad.

2. Funciones Hash

    - Algoritmos que crean mensajes (digeridos) "digests" únicos, usados principalmente para validar la integridad.

3. Firma digital

    - Algoritmos que aseguran el origen del mensaje, atendiendo el problema de la autenticación.

Tal y como comenta Preukschat (2014) en su artículo para la revista "oroyfinanza.com: ¿Qué es y de qué sirve el algoritmo SHA-256 en el protocolo bitcoin?"[5], un algoritmo de encriptación (o cifrado) tradicional es una función que transforma un mensaje en una serie ilegible aparentemente aleatoria, usando una clave de encriptación que puede ser revertida (es decir, obtener el mensaje original) sólo por quienes conocen dicha clave. Por medio de la encriptación, la información privada puede ser enviada públicamente por internet sin mayor riesgo de que otros puedan tener acceso a ella. A lo largo de la historia los algoritmos de encriptación se han vuelto más recurrentes. Hoy con el uso de sistemas globalizados son usados ampliamente para el resguardo de la información. Sin el uso de este tipo de técnicas el robo de información se centraría en su obtención y no presentaría mayores retos al ladrón para su aprovechamiento malicioso.

Según el artículo publicado por Delgado y Palacio (2006) para la web de "icai.es", en la criptografía las funciones hash (o función resumen) es una función que transforma cualquier número o serie de caracteres (entrada) en un resultado de tamaño fijo (valor hash), pero no permite revertir el proceso fácilmente. Para hacerlo, para determinar la entrada a partir del valor hash, es necesario probar con todas las posibles entradas. Podemos ver un ejemplo de una función hash a partir de una raíz cuadrada: la raíz cuadrada de 17.202 es fácil de calcular (alrededor de 131.156351921463). Una simple función hash, entonces, puede ser los últimos 7 dígitos del resultado así obtenido (en este caso, 921463). Contando solo con este dato es muy difícil averiguar el número inicial del que éste provino y, básicamente, uno debería pasar por todas las posibilidades para determinarlo, pero quien conozca la cifra inicial podrá reproducir el valor hash muy fácilmente.

Como explica Delgado y Palacio (2006), los hashes criptográficos modernos, como el SHA-256 que utiliza Bitcoin, son una versión mucho más segura y compleja de esto. En general estas funciones se usan para verificar la integridad de la información, ya sea para detectar errores o intentos malintencionados.

Por otro lado, el bitcoin usa la firma digital basada en criptografía de clave pública para autenticar datos y verificar correctamente quién está autorizado a transferir monedas, permitiendo además identificar la falsificación y la manipulación de su contenido. Más concretamente, es un método de cifrado en el que toda clave privada tiene una clave pública correspondiente, a partir de la cual es imposible determinar la clave privada. Nos permite publicar una clave que cualquiera puede usar para enviarnos un mensaje cifrado sin que tengamos que compartir nuestra clave privada. En general

[5] Consultado el 26/06/2017 en https://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm/

los algoritmos que usan la firma digital pueden asegurar que la información no contiene errores, no ha sido modificada y que el emisor de dicha información es el propietario de la misma. En resumen la:

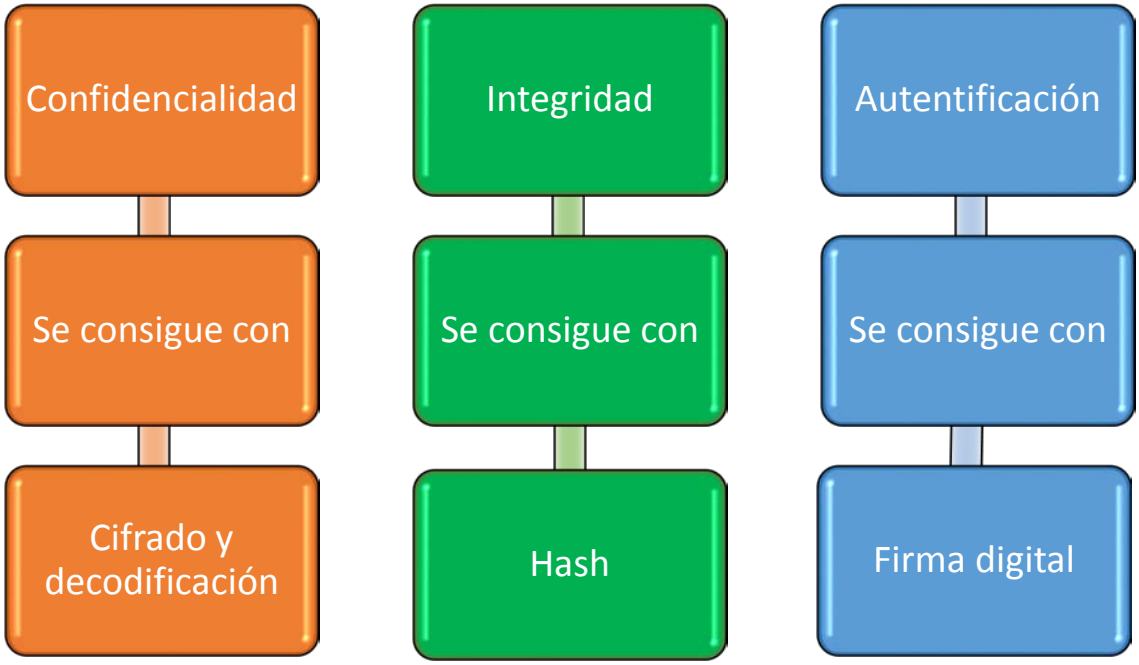

Figura 1. Los tres aspectos importantes de la criptografía.
Fuente: Elaboración Propia.

2.2.2 Blockchain

Además de la criptografía, la mecánica del bitcoin se fundamenta también en tecnología del blockchain. Como explica Márquez (2016), lo primero es que cada nuevo usuario debe elegir un monedero, que es un programa informático, e instalarlo en su ordenador o en su dispositivo móvil; cada monedero posee una llave especial creada con algoritmos de criptografía que se emplea para realizar firmas digitales y que verifican la identidad del usuario.

Tras este primer paso, se origina una dirección de Bitcoin (pudiendo crearse cuantas se necesiten ya que las direcciones Bitcoins solamente deberían ser usadas una única vez), que se enviará a otros usuarios para proceder a pagos o transferir Bitcoins.

En tercer lugar, las transferencias se verifican por medio de un registro de contabilidad público denominado “block chain” (“cadena de bloques”), que muestra todas las transacciones confirmadas y asegura que el usuario posee la cantidad de bitcoins que pretende gastar. Cada equipo informático que participa en la red es lo que se conoce como nodo. No hay un servidor, no hay un servicio centralizado, y no hay una jerarquía dentro de la red.

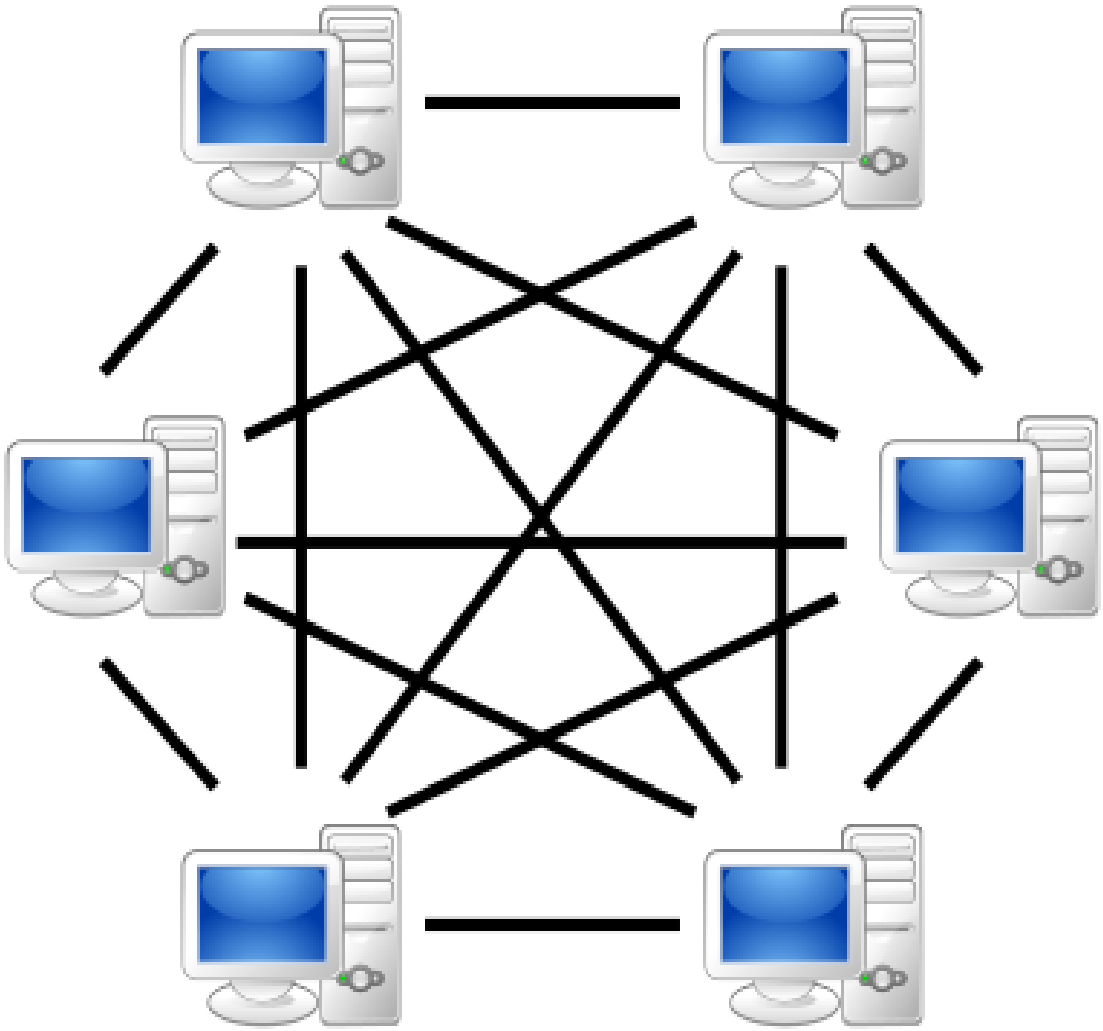

Figura 2. Red peer to peer.
Fuente: under-linux.org.

Según Antonopoulos (2014, pag 35), la red Bitcoin implica, por tanto, una red de ordenadores en todo el mundo que constantemente retransmite y transmite nuevas transacciones entre sí. Cada ordenador en esta red es un nodo que tiene descargado la blockchain (cadena de bloques). Cualquier persona puede ser un nodo en la red bitcoin. Basta con instalarse el Bitcoin Core, al igual que instalamos cualquier tipo de software en nuestro ordenador y, una vez finalizada la instalación, tu ordenador se convierte en un nodo más de la red bitcoin.

Una vez explicado que es un nodo, se procede a comentar la función de la cadena de bloque, que es la tecnología que emplea el bitcoin, pero que puede ser empleada por muchos otros sistemas informáticos. Tal y como se hace mención en el blog de “bit2me.com” en palabras de Marc Andreessen, creador de Netscape y socio de uno de los fondos de Capital Riesgo más importantes de Silicon Valley:

“Una cadena de bloques es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está “distribuido” o es compartido entre muchas partes diferentes”.

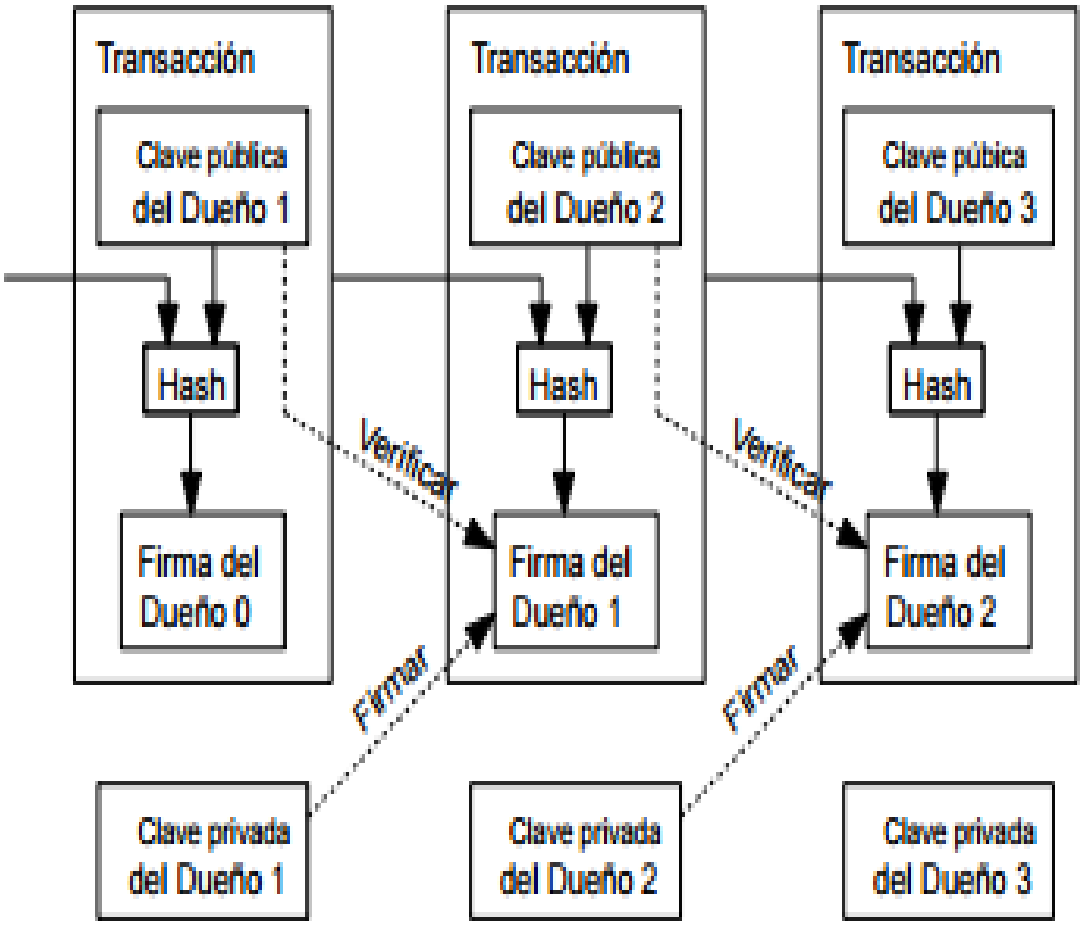

Figura 3. Cadena de bloques (Block Chain).
Fuente: puntodevistaeconomico.wordpress.com

Tal y como expresa González (2013, pag 32), cualquier transacción transmitida a otros nodos no se convierte inmediatamente en “oficial”; primero tiene que ser confirmada en una lista –mantenida colectivamente- de todas las transacciones conocidas: cadena de bloques.

Siguiendo con Márquez (2016), la integridad y el orden cronológico de la cadena de bloques se hacen cumplir con la criptografía. Después, a través del “mining” (“minería”), se transmiten y confirman las transacciones pendientes de ser incluidas en la cadena de bloques, elemento que explicaremos con más detalle en su aplicación en el bitcoin.

Este proceso hace cumplir un orden cronológico en la mencionada cadena, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones deberán ser unidas en un bloque que se ajuste a estrictas normas de cifrado y que será verificado por la red, lo que impedirá que cualquier bloque anterior se modifique (lo que invalidaría todos los bloques siguientes). En definitiva, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de esta para revertir sus propios gastos, por eso el bitcoin se fundamenta en una tecnología de producción de moneda de forma descentralizada, mediante el sistema de blockchain.

CAPÍTULO 3

FUNCIONAMIENTO DEL BITCOIN

3.1. OBTENCIÓN DE LOS BITCOINS

Existen dos formas para que un agente económico consiga Bitcoins. Una de ellas es mediante la realización de transacciones económicas de diversa índole, al igual que con cualquier otra moneda, y la segunda es la producción o "minería de bitcoins".

Como se ha comentado, lo primero es elegir ese monedero de Bitcoins donde guardar el valor de las criptomonedas. Los monederos, carteras o Bitcoin wallets (González; 2013, pag 147), es en realidad un archivo que necesitamos para enviar y recibir Bitcoins; puede decirse que este archivo "contiene" nuestros Bitcoins, aunque en realidad lo que contiene son llaves criptográficas (claves privadas, únicas, irrepetibles y secretas) que nos hacen dueños de nuestros Bitcoins y nos permiten autorizar pagos (transferir la posesión de nuestros Bitcoins).

Una vez elegido un monedero digital donde guardarlos, existen diversas formas de obtener las criptomonedas a través de transacciones económicas (González, 2013, p.149):

- Sitios de compra-venta de Bitcoins. El más utilizado es MtGox. Pero hay muchos otros sitios que facilitan el intercambio de todo tipo de divisas por bitcoin y admiten diversos sistemas para transferir los fondos. "Bitinstant" y "Bitcoin-Nordic" venden Bitcoins a través de cientos de miles de puntos de venta distribuidos en todo el mundo.

- Sitios que aceptan oro o plata a cambio de Bitcoins: ejemplo de ello es "coinabul".

- Aceptar Bitcoins como pago por bienes o servicios. Es posible fijar un precio en cualquier moneda y optar por ajustar automáticamente los precios nominados en Bitcoins, para que el coste de los productos no se vea afectado por las fluctuaciones en el tipo de cambio. Por medio de "Bit-Pay", los pagos en Bitcoins además pueden ser automáticamente convertidos a la moneda que el comerciante prefiera.

- Encontrar personas dispuestas a vender Bitcoins: se pueden localizar por medio de "tradebitcoin.com", "localbitcoins.com" o foros especializados, entre otros sitios. En general se trata de "antiguos" mineros que disponen de grandes cantidades de Bitcoins, aunque también hay operadores que compran Bitcoins y los venden cobrando una comisión.

- También hay empresas que pagan Bitcoins por determinadas acciones que haga el usuario, como ver publicidad en webs o jugar a juegos basados en Bitcoins.

La segunda vía es la producción mediante la "minería de bitcoins", pero antes de explicarla es necesario definir y explicar el funcionamiento de la minería. La web de bitcoin "bitcoin.org" lo define como el proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados. Podría describirse como el centro de datos de bitcoin, excepto que este ha sido diseñado para ser completamente descentralizado con "mineros" operando en todos los países y sin que nadie tenga el control absoluto sobre la red. Este proceso se denomina "minería", como analogía a la minería del oro, ya que

también es un mecanismo temporal utilizado para emitir nuevos bitcoins. No obstante, a diferencia de la minería del oro, la minería de Bitcoin ofrece una recompensa a cambio de servicios útiles que son necesarios para que la red de pagos funcione de manera segura. La minería de Bitcoin seguirá siendo necesaria hasta que se haya emitido el último bitcoin.

Según el artículo publicado por Valkenburgh (2014) para la web "coincenter.org: What is bitcoin mining, and why is it necessary?"[6], los bitcoins no son enviados y recibidos como archivos adjuntos en un correo electrónico. No hay archivos en absoluto, solo las asignaciones de bitcoins hechas a varias direcciones públicas. Cada dirección pública tiene una clave privada correspondiente y solo el titular de esa clave es capaz de firmar digitalmente una nueva solicitud de transacción. Además, la solicitud debe tener inputs. Los inputs son las transacciones anteriores que el remitente está utilizando para financiar la nueva transacción. Si ha recibido previamente cinco bitcoins de Alice y cuatro de Bob, puede juntar estos inputs para financiar una nueva transacción a Cynthia por valor de hasta nueve bitcoins.

Los mineros comprueban dos cosas cuando reciben una solicitud. Primero comprueban que realmente la firma digital ratifica que hayas sido anteriormente el destinatario de dichos inputs. En segundo lugar, comprueban para asegurarse de que no hayas gastado ya esos inputs. Para realizar esta segunda comprobación, los mineros "*pican",* terminología empleada por analogía con la minería para indicar que realizan una labor de comprobación*,* en la cadena de bloques, de todas las transacciones válidas ya efectuadas, para ver si esos inputs ya se utilizaron en una transacción o si todavía están disponibles. Las copias de la cadena de bloques se almacenan en los equipos informáticos de todos los usuarios de Bitcoin que se conectan a la red.

Por lo tanto, los mineros desempeñan el papel de los cajeros de banco: inspeccionan los cheques, asegurándose de que todas las firmas correspondientes y números de cuenta están correctos, comprobando la identidad del cliente, y buscando pruebas de que el cliente tiene suficiente efectivo para realizar la transacción.

Si todo sale bien, el minero añadirá la transacción a su lista personal de todas las transacciones válidas en los últimos minutos. Cada pocos minutos, se seleccionará un minero para agregar su lista personal, un bloque, a la cadena de bloques oficial, manteniendo así el registro público actualizado.

Para evitar que un minero de manera fraudulenta corrompa la cadena de bloques, el protocolo bitcoin fuerza que los mineros tengan que competir. Un minero diferente está facultado para completar cada bloque, aproximadamente cada 10 minutos, y sólo los bloques válidos serán validados por el resto de la comunidad minera. He aquí cómo funciona:

Siguiendo con Valkenburgh (2014), un bloque de un minero se convertirá en una parte de la cadena cada vez que una mayoría de la comunidad de mineros lleguen al consenso de que:

- Las transacciones registradas por el minero sean válidas, sin firmas de imitadores y sin doble gasto.
- Que el minero haya adivinado correctamente un número especial, el "Nonce", que resuelve un problema matemático particular. Los mineros realizan esta comprobación examinado la firma digital particular del bloque propuesto. Esta firma es un producto generado por el ordenador con tres entradas:
    1. La firma del bloque anterior.

[6] Consultado el 26/06/2017 en https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary

2. Una lista de las transacciones válidas desde el anterior bloque.
3. Un número aleatorio particular, el llamado “Nonce”.

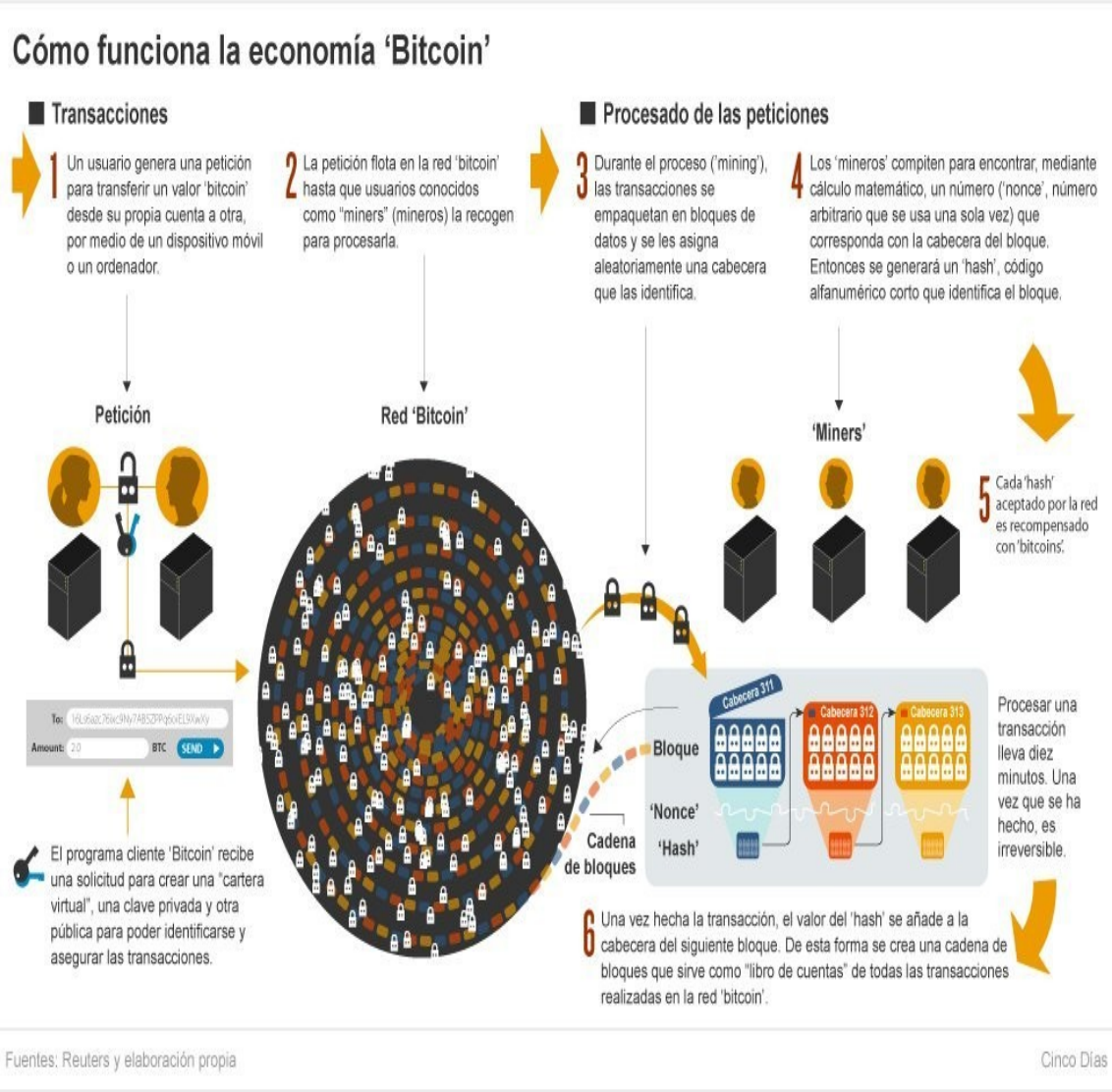

Figura 4. Funcionamiento de la economia del Bitcoin
Fuente: https://www.weforum.org/es/agenda/2017/04/blockchain-la-revolucion-pendiente-de-internet?utm_content=buffer4d903&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

La práctica del minado de bitcoin consiste en: aquel que sea el primero en “producir” (encontrar) un nuevo bloque, recibirá Bitcoins a modo de recompensa por su trabajo. Esto es lo que el proceso de minería ha llamado como “prueba de trabajo” (Back, 2002)[7]

Según González (2013, pag 34), la cantidad de bitcoin creada por lote nunca es ni será mayor a 50 bitcoins, y los premios (el número de bitcoins por lote) están programados para disminuir con el paso del tiempo, reduciendo el incremento de la masa monetaria de manera predecible, hasta llegar a cero, pues así lo estableció Satoshi. Nunca llegarán a existir más de 21 millones de bitcoins. Así se muestra en la Figura 5. En el pasado año, unas 25.000 personas que realizaban esta tarea, generaban

[7] Consultado el 26/06/2017 en http://www.revista.unam.mx/vol.18/num1/art11/art11.pdf

unos 25 Bitcoins cada 10 minutos, cantidad que se redujo a la mitad a finales del 2016 y que seguirá reduciéndose un 50% cada 4 años, por lo que esta práctica para conseguir divisa virtual cada vez es más complicada.

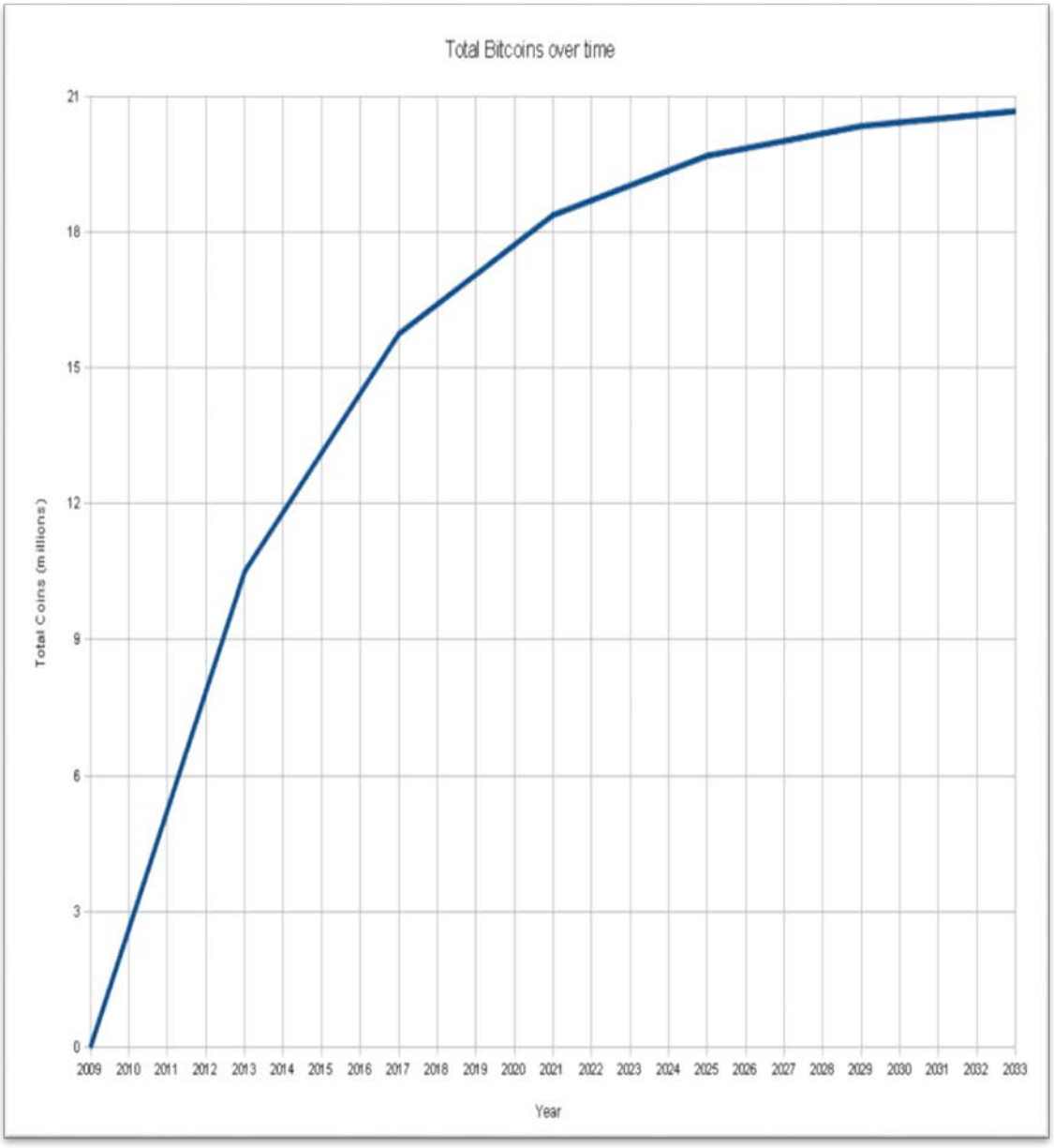

Figura 5. Previsión del número total de Bitcoin en el tiempo.
Fuente: https://es.wikipedia.org/wiki/Bitcoin

En la Figura 6 se observa cómo ha ido incrementando el número total de bitcoins desde su lanzamiento hasta el, 26 de junio de 2017, cuyo número está en 16.412.875 bitcoins

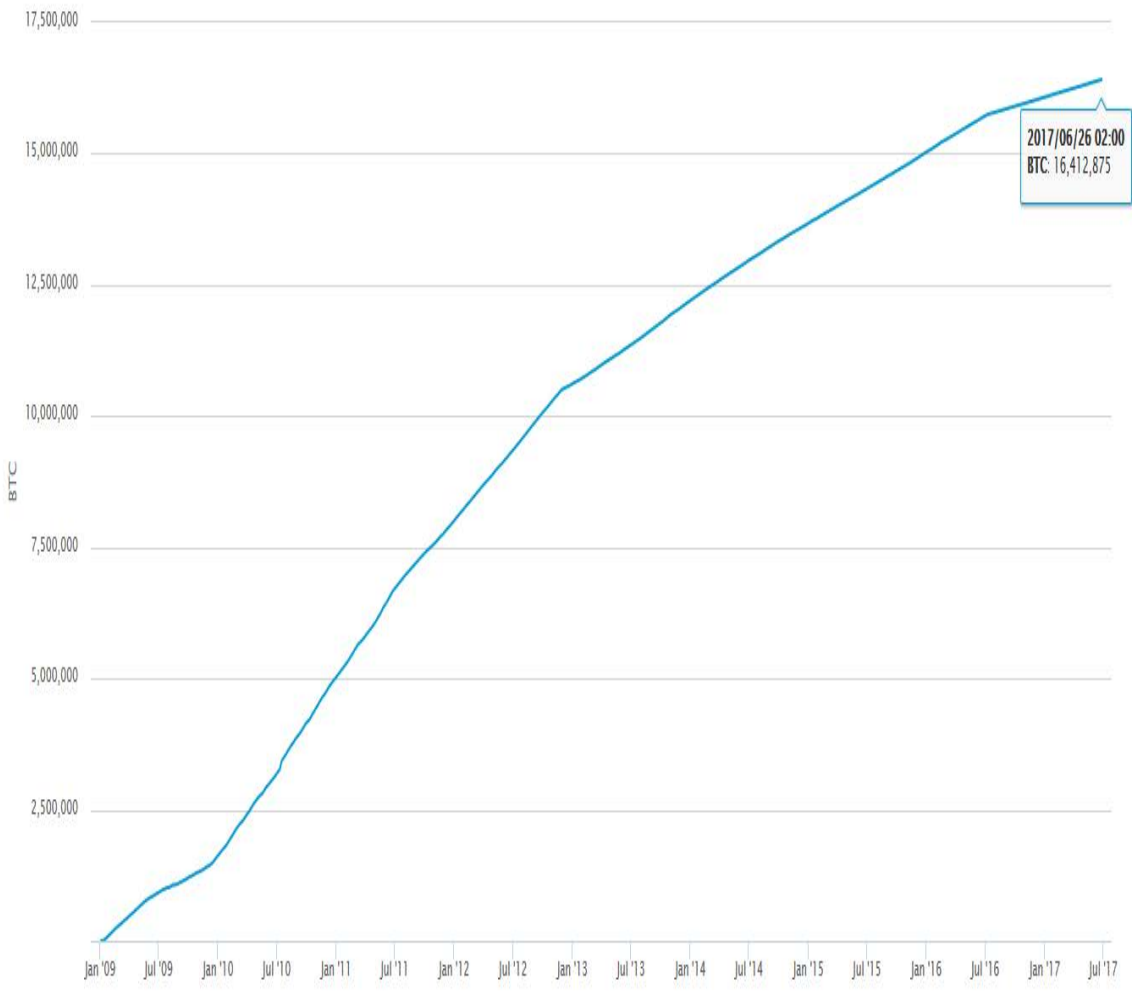

Figura 6. Total de Bitcoins en circulación.
Fuente: https://blockchain.info/es/charts/total-bitcoins?timespan=all

3.2. PRINCIPALES MONEDEROS

Según Márquez (2016), el bitcoin opera bajo tecnología peer-to-peer, o lo que es lo mismo, equipos iguales entre sí, para así evitar depender de una autoridad monetaria central que se encargue de la emisión y el control de dinero. Así, no es posible manipular el valor de los Bitcoins o crear inflación produciendo más moneda. La propia red es la que gestiona las transacciones y la emisión de Bitcoins, que se generan a través de la llamada minería, de forma controlada y descentralizada, no siendo controlada por ningún Estado, institución financiera, banco o empresa. Se trata de una moneda intangible, aunque puede ser utilizada como medio de pago igual que el dinero físico. La utilización de criptografía garantiza la seguridad de las transacciones. Por ejemplo, se puede controlar que sólo el dueño de las monedas pueda gastarlas, y que sólo las pueda utilizar en una única transacción.

Siguiendo con Márquez (2016), para evitar que un mismo Bitcoin sea gastado más de una vez por la misma persona (en otras palabras, para evitar la falsificación), la red se vale de lo que se describe como un servidor de tiempo distribuido, que identifica y ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de pruebas de trabajo encadenadas (las cuales se muestran como “confirmaciones”).

Si bien el envío de Bitcoins es instantáneo, y cualquier operación puede ser monitoreada en tiempo real, las confirmaciones que nos muestra la pantalla cuando usamos el software de Bitcoin vienen a representar el proceso de clearing (compromiso de una transacción hasta ser establecida). A mayor número de confirmaciones, más remota será la posibilidad de ser víctima de un doble gasto. Cuando supera las cinco confirmaciones por parte de la red, una transacción es considerada técnicamente irreversible

Tal y como se ha comentado antes, existen varios tipos de monederos Bitcoins. Monederos de escritorio, de móvil o de web, para todos ellos es necesaria la descarga de la aplicación que posee los Bitcoins para realizar las operaciones.

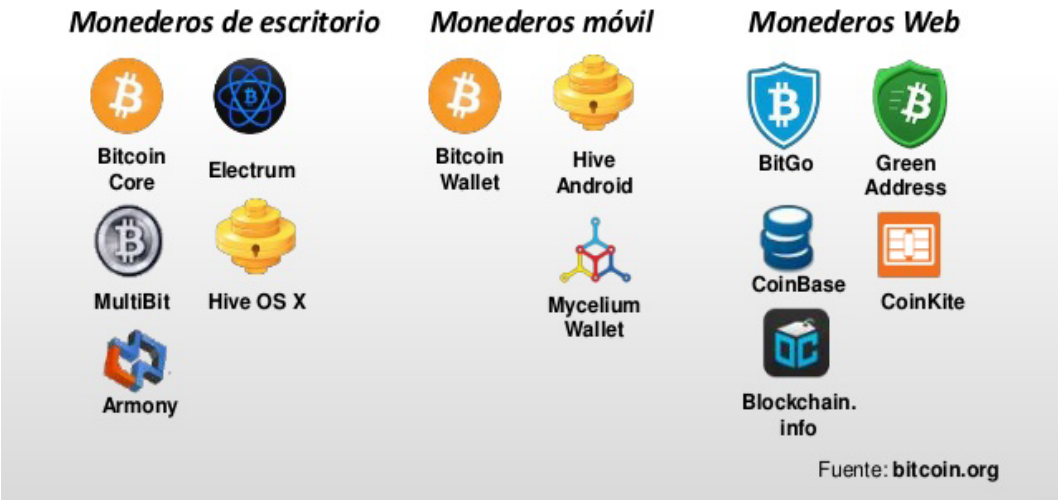

Figura 7. Tipos de monederos Bitcoins.
Fuente: bitcoin.org.

A continuación se detallan los más utilizados según Márquez (2016):

- BlockChain; Cuenta con una innovadora página, de manejo fácil y seguro para todos los usuarios y empresas alrededor del mundo. En la actualidad (26 de junio de 2017) cuenta con cerca de 15 millones de usuarios registrados y está teniendo un gran crecimiento en estos últimos años, tal y como se observa en la Figura 8.

  Principales características de Blockchain según la web tudineroasegurado.com"[8] son:

  - Es completamente gratis y no cuenta con tarifas de manejo.
  - Cuenta con seguridad de Autenticación de dos factores.
  - Constantes actualizaciones del monedero.
  - Podrás hacer tus propias copias de seguridad.
  - Posibilidad de importar o exportar tus clases privadas.
  - Notificaciones a través de SMS y correo electrónico.

[8] Consultado el 28/06/2017 en https://www.tudineroasegurado.com/cual-es-el-mejor-monedero-de-bitcoin/

- Dispone de una App para teléfonos móvil.
- Fácil e intuitivo manejo.
- Cuenta con una amplia red de mercado que aceptan Bitcoin como medio de pago.

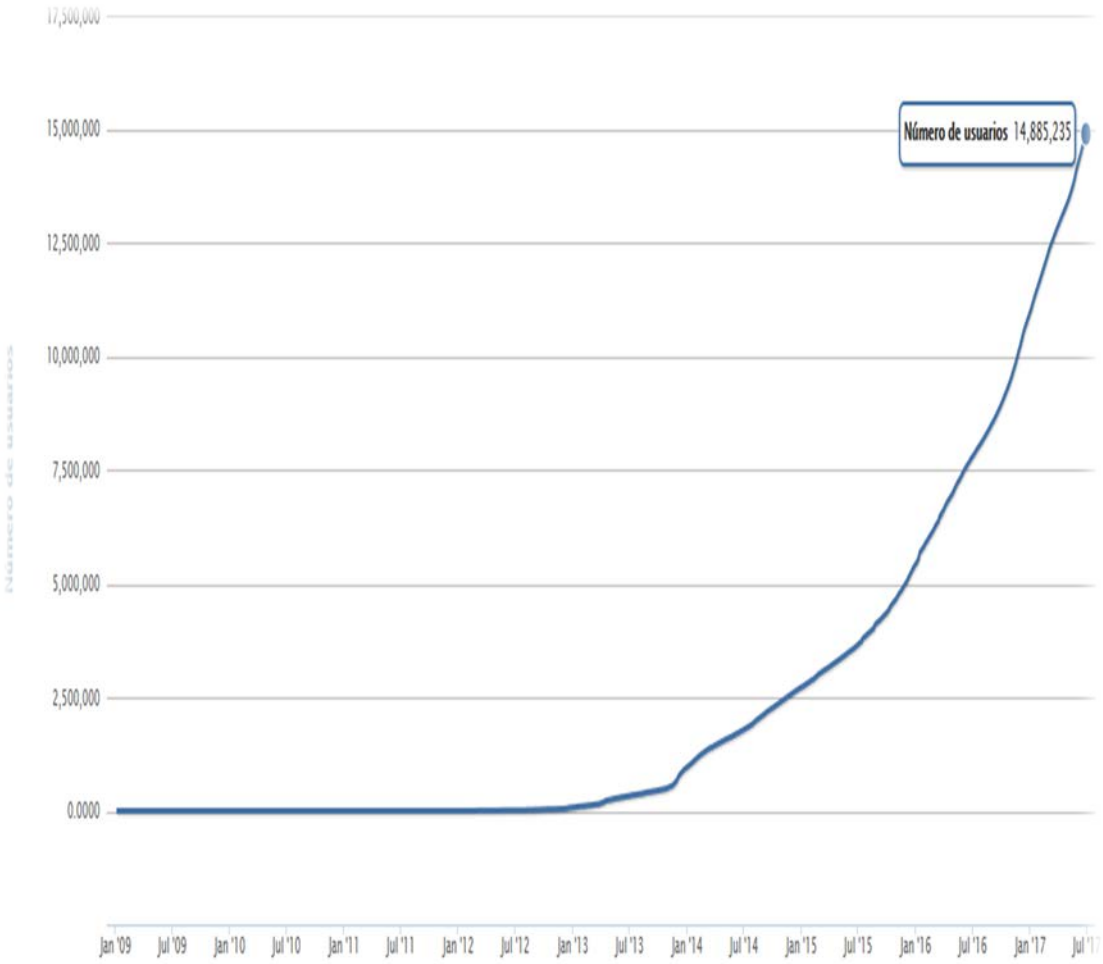

Figura 8. Número de usuarios Blockchain.
Fuente: https://blockchain.info/es/charts/my-wallet-n-users

- MultiBit; Muy recomendado para usuarios con pocos conocimientos técnicos y para aquellos usuarios que deseen operar con Bitcoins rápidamente sin ningún tipo de miramientos o complicaciones.

  Principales características de MultiBit según el "blog.bit2me.com: Monederos bitcoin ligeros para ordenador: Multibit y Electrum"[9] son:

  - Una de sus características más importantes es que permite al usuario realizar copias de seguridad de forma muy sencilla ya que tan sólo tiene que guardar una semilla formada por un conjunto de caracteres que puede importar en cualquier otro monedero sin requerir más información.

[9] Consultado el 28/06/2017 en http://blog.bit2me.com/es/monederos-bitcoin-ligeros-para-ordenador/

  - No soporta ningún tipo de coste.
  - capacidad de abrir varios monederos a la vez.
  - Multiplataforma: funciona tanto en Windows como Linux y OS X.
  - Seguro: los datos se mantienen cifrados en la máquina del usuario.
  - Traducida en más de 40 idiomas.
  - Descentralizada y sin servidores fijos.
  - Instalación en 5 minutos.

- Coinbase; Cuenta con el apoyo de muchos inversores a nivel mundial donde destaca el Banco BBVA, el cual inyectó un gran capital por el gran potencial que tiene esta página. Actualmente tiene más de 8 millones de usuarios registrados.

  Principales características de Coinbase según la web "tudineroasegurado.com"[10] son:

  - Monedero completamente Gratis y sin cuotas de manejo.
  - El usuario podrá comprar y vender Bitcoin al público.
  - Constantemente actualizada y segura.
  - Cuenta con la opción de poder hacer copias de seguridad.
  - Tiene a disposición una caja fuerte de manera gratuita con seguridad extra.
  - Cuenta con notificaciones a través de SMS y correo electrónico sobre movimientos.
  - Cuenta con App para teléfonos móvil.
  - Fácil de usar y muy intuitivo.
  - Cuenta con una amplia red de mercado que acepta Bitcoin como medio de pago.
  - El usuario podrá hacer retiros programados si así lo deseas.

- Bitcoin Core; Conocido como el monedero original, cuando Satoshi Nakamoto creó los bitcoins utilizó un primer monedero virtual, y ese fue el Bitcoin Core, anteriormente llamado Bitcoin-Qt. Es el monedero virtual más antiguo, pero también el más seguro gracias a que mantiene continuas actualizaciones que ofrecen una gran cantidad de características de seguridad y privacidad, y admite una completa transparencia.

  Para muchos no es el monedero virtual de bitcoin más fácil de usar, pero sin duda estamos delante del mejor, y lo más importante es que es multiplataforma.

  - Ofrece un sistema altamente estable.

[10] Consultado el 28/06/2017 en https://www.tudineroasegurado.com/cual-es-el-mejor-monedero-de-bitcoin/

  - Cartera mucho más segura que las wallets ligeras porque descarga toda la cadena de bloques.

  - Las claves privadas se almacenan dentro del ordenador en un archivo que se llama **"**wallet.dat" por lo que ofrece mucho más seguridad que los monederos online, donde las claves se almacenan en la nube.

  - Es el único programa que implementa totalmente el protocolo Bitcoin, protegiendo la red, y se considera la referencia en la que se apoyan el resto de clientes existentes.

- Electrum. Se centra en la velocidad y simplicidad con un bajo uso de recursos. Es uno de los monederos ligeros más utilizados por su sencilla configuración.

  Las principales características de Electrum según "blog.bit2me.com: Monederos bitcoin ligeros para ordenador: Multibit y Electrum"[11] son:

  - Almacenamiento seguro de Bitcoin usando una computadora fuera de línea.

  - Monedero totalmente gratis, sin ningún coste de servicio.

  - Claves privadas cifradas en el ordenador por lo que ningún tercero tendrá acceso a ellas por defecto.

  - Posibilidad de exportar las claves privadas y utilizarlas en cualquier otro monedero.

  - Es un monedero para Mac, Linux, y Windows.

- Mycelium; Monedero diseñado para ofrecer seguridad, rapidez y un uso fácil. Su administración de direcciones es lo que hace que sea una de las mejores aplicaciones de monedero bitcoin. Según su página web "mycelium.com" le fue concedida el premio a la "Best Mobile app" de Blockchain.info en 2014.

  Las principales características de Mycelium según "criptonoticias.com (2016): usando la cartera de bitcoin mycelium"[12] son:

  - Ofrece un control total al usuario sobre sus llaves privadas. Nunca estarán fuera de su aplicación a menos que las exporte.

  - Es una billetera totalmente gratis.

  - Su servidor privado centralizado se encargará de manejar todas las transacciones de forma segura.

  - Como su código fuente es libre, cualquier desarrollador puede auditar el código y decidir si le parece una aplicación segura o no.

  - Al correr en dispositivos móviles, se tiene la seguridad de que ningún spyware podrá tener acceso a la aplicación.

[11] Consultado el 28/08/2017 en http://blog.bit2me.com/es/monederos-bitcoin-ligeros-para-ordenador/

[12] Consultado el 28/06/2017 en https://criptonoticias.com/tutoriales/tutorial-usando-cartera-bitcoins-mycelium/#axzz4lEiEJKo6

3.3. DIRECCIONES

Tal y como se define en la web “Bitcoinwiki.com”, una dirección Bitcoin, o simplemente dirección, es un identificador de entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3, que representa un destino de un pago en Bitcoins. Ejemplo de una dirección Bitcoin es:

Figura 9. Dirección de Bitcoin.
Fuente: colombia-mmm.net.

Las direcciones se pueden generar muy fácilmente y en número arbitrario desde cualquier programa cliente de Bitcoin.

Según González (2016, pag 31), cualquier persona que participa en la red Bitcoin posee una billetera electrónica que contiene pares de llaves criptográficas (pública/privada). Las direcciones visibles derivan de las llaves públicas de cada usuario, las cuales, no tienen ninguna información sobre sus dueños y a su vez funcionan como los puntos remitente/receptor para todos los pagos. Las llaves privadas correspondientes a cada llave pública sirven para que un determinado usuario autorice pagos (transfiera Bitcoins) desde su billetera. En definitiva, estableciendo una analogía con cuentas bancarias, la clave pública (la dirección) sería el número de cuenta, y la clave privada sería la contraseña de la cuenta.

Como se ha comentado anteriormente, los usuarios de Bitcoins pueden tener múltiples direcciones; pudiendo generar direcciones nuevas fácilmente y sin límites, como es el caso de la Figura 10.

Figura 10. Direcciones de Bitcoins.
Fuente:https://es.wikipedia.org/wiki/Bitcoin#/media/File:Screenshot_of_Bitcoin-qt-0.5.2.png.

Siguiendo con González (2016, pag 32), generar una nueva dirección equivale a generar un nuevo par de llaves (pública/privada). Los usuarios que desean preservar el anonimato suelen crear una nueva dirección para cada transacción.

3.4. TRANSACCIONES

La web de “Bitcoinwiki.com” define una transacción como una sección de datos con firma digital que se transmite a la red y se almacena en los bloques. Este conjunto de datos incluye una referencia a una transacción anterior e indica una cantidad de bitcoins que pasan a estar disponibles para una dirección Bitcoin de destino.

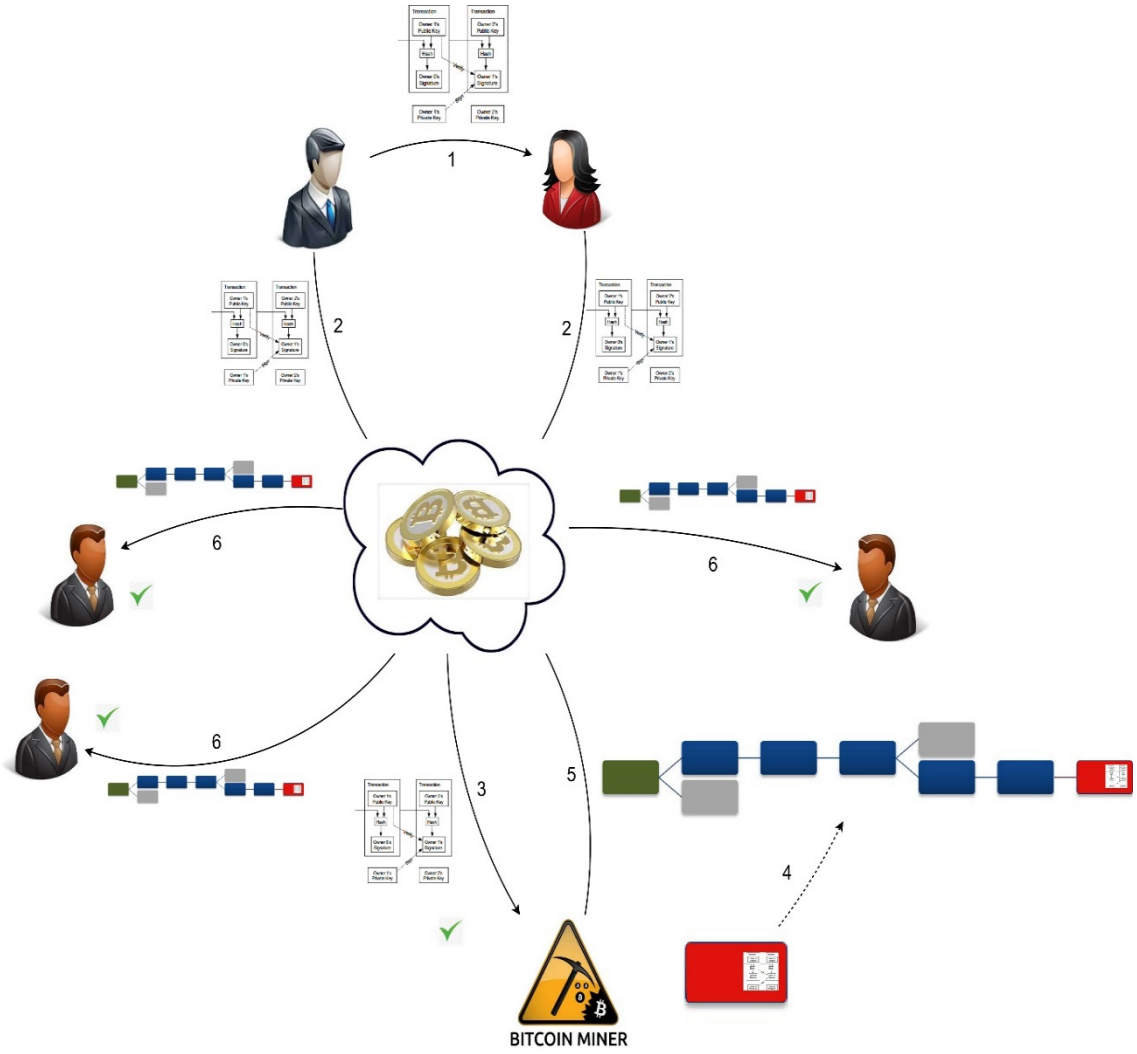

Figura 11. Diagrama de una transacción de Bitcoins.
Fuente: www.incibe.es.

Antes de explicar cómo funciona la transferencia de Bitcoins de una persona a otra, se hará una pequeña mención a los participantes que actúan en el sistema Bitcoin, los cuales son dos:

- Usuarios: compran y venden utilizando bitcoins, generando y publicando las transacciones correspondientes.

- Mineros: reciben transacciones de otros usuarios, las verifican, y trabajan para incluirlas en la cadena de bloques de transacciones aceptadas.

A continuación se emplea la Figura 11 para explicar con más claridad el funcionamiento general de un pago con bitcoins.

1. Bob hace un pago en bitcoins a Alice.
2. Alice y Bob envían la transacción a la red P2P de Bitcoin.
3. Un minero recibe la nueva transacción y la verifica.
4. El minero encuentra un bloque válido que incluye la nueva transacción.
5. El minero envía el nuevo bloque a la red P2P de Bitcoin.
6. El resto de usuarios de Bitcoin actualizan su cadena, verificando que el nuevo bloque es válido.

Cuando Bob transfiere bitcoins a Alice, Bob renuncia a la posesión de un determinado número de bitcoins, agregándoles la llave pública de Alice y firmando la combinación resultante con su llave privada con el fin de demostrar que está de acuerdo con la transacción realizada.

Tal y como se expresa en la web “elbitcoin.org”, cada nodo generador de bitcoins recoge todas las transacciones que aún no fueron confirmadas en un archivo (el bloque candidato) que contiene la referencia a dichas transacciones y al último bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un hash de ese bloque (un código aleatorio que lo representa), en un esfuerzo computacional que demanda cantidades predecibles de intento y error. Cuando un nodo encuentra la solución, la transmite a toda la red. El resto de nodos reciben el nuevo bloque solucionado, lo verifican antes de aceptarlo y lo agregan a la cadena. Tal es el trabajo de los nodos generadores, cuyos dueños son los mineros de Bitcoins.

Siguiendo con esta web, ningún usuario de bitcoin está forzado a revelar su identidad, todas las transacciones jamás realizadas quedan grabadas en esa base de datos de libre acceso que es la cadena de bloques. Esta contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de bitcoin. Por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó (doble gasto), la red lo detectará y rechazarán la transacción.

A continuación se muestra en la Figura 12 el número de transacciones por bloques realizadas desde que bitcoin está en funcionamiento hasta fecha de 26 de junio de 2017, cuyo número era de 1844 transacciones por bloque.

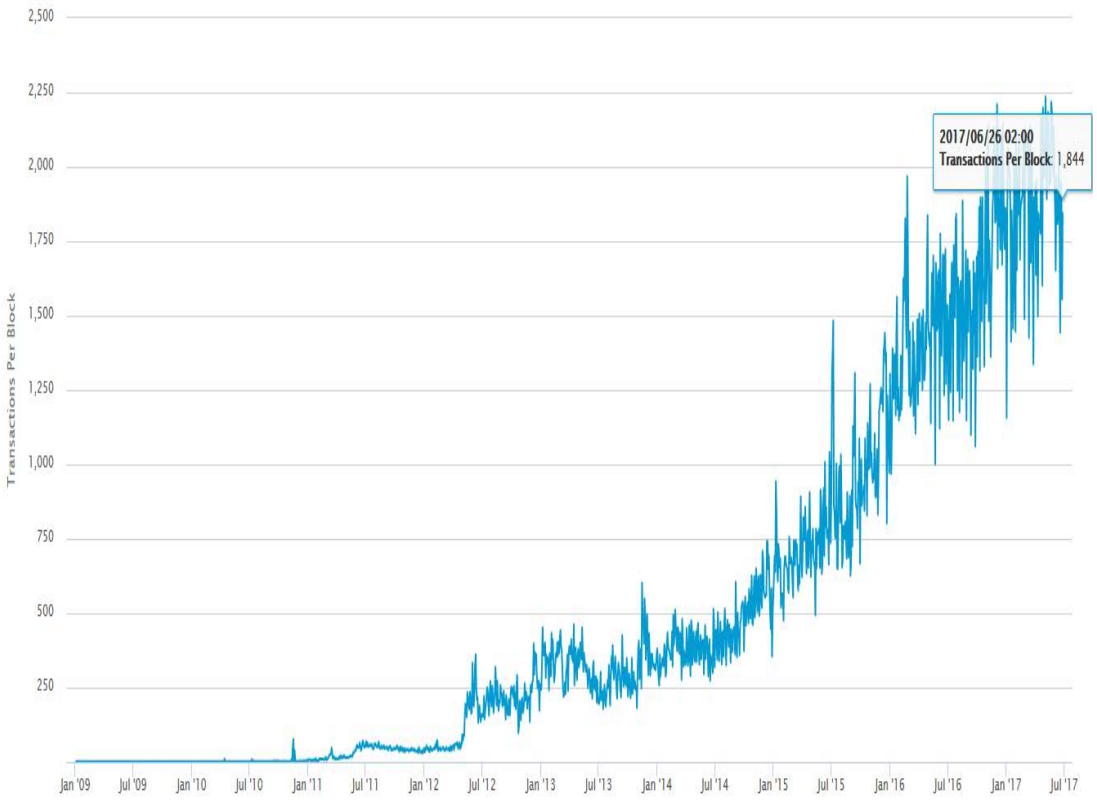

Figura 12. Número de transacciones por bloque.
Fuente: https://blockchain.info/es/charts/n-transactions-per-block?timespan=1year

Según González (2013, pag 33), la cadena de bloques es un registro totalmente transparente: cualquiera puede examinarla, en cualquier momento, para informarse acerca de cualquier transacción que se haya realizado desde el lanzamiento de bitcoin, un 3 de enero de 2009, así como de las nuevas transacciones que se van agregando a la cadena en tiempo real. Varios servicios facilitan este tipo de monitoreo.

En definitiva, de la creación de nuevos bloques se encarga la minería, labor que realizan personas, llamadas “mineros”, repartidos por el planeta, que ponen a disposición del sistema bitcoin, el poder computacional de sus máquinas y ordenadores.

Desde el punto de vista de la red, los mineros proveen seguridad al sistema, verificando las transacciones que se llevaron a cabo e impidiendo que haya errores de cómputo y crédito.

A continuación, en la Figura 13 se muestra el número de transacciones realizadas a lo largo de la vida de bitcoin hasta el 26 de junio de 2017, el cual es de 235.127.209, así como en la Figura 14 el número de transacciones realizadas por día en la actualidad es de 261.906

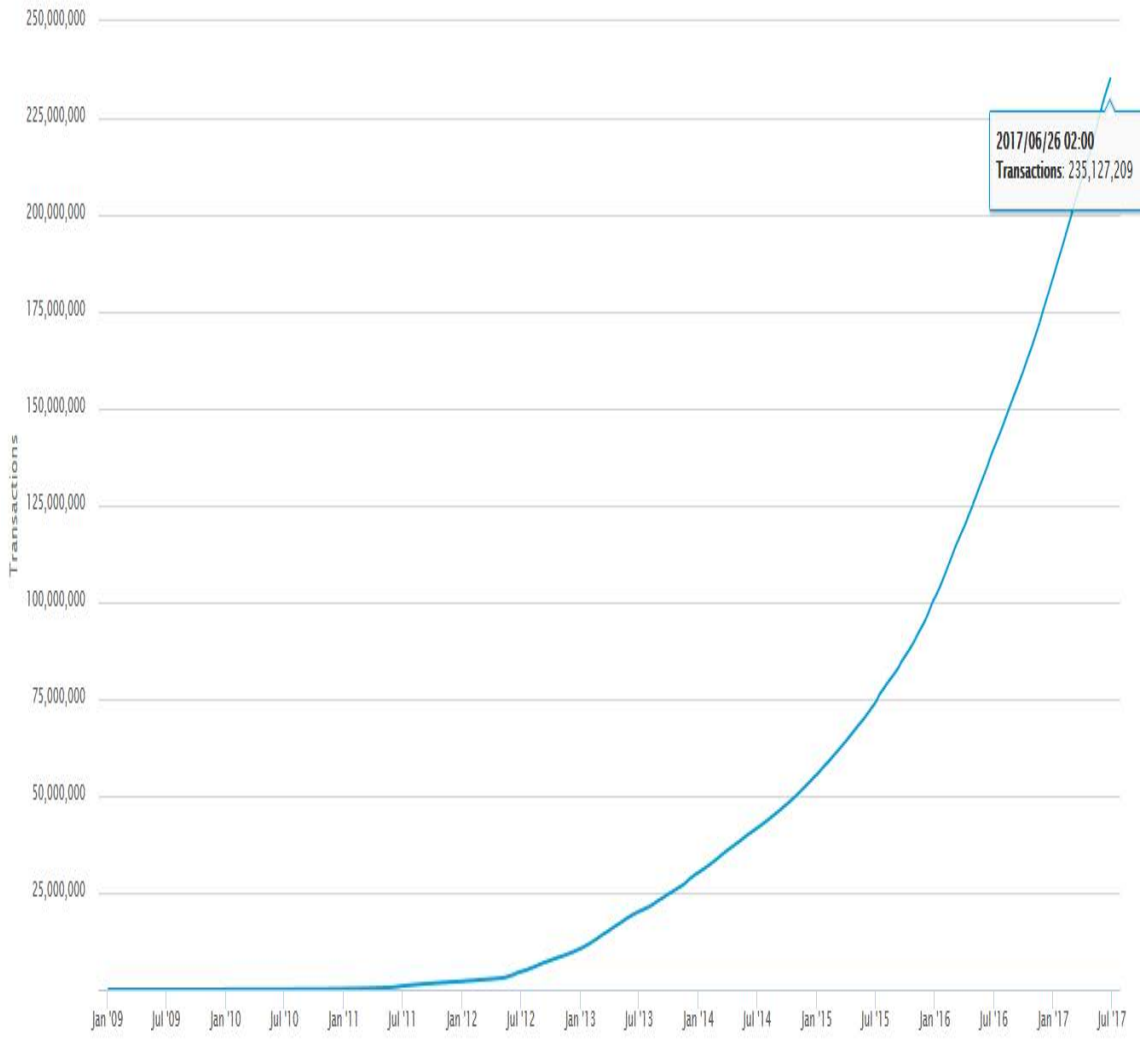

Figura 13. Número total de Transacciones
Fuente: https://blockchain.info/es/charts/n-transactions-total

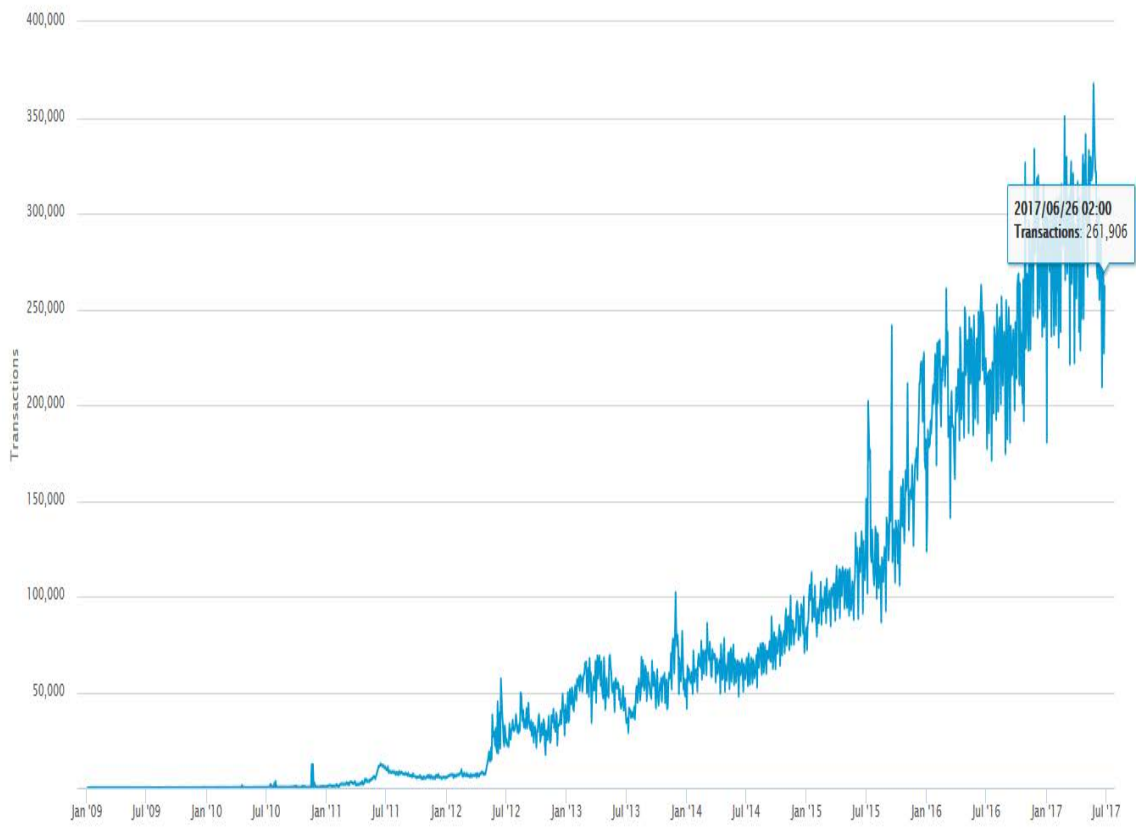

Figura 14. Número de transacciones por día
Fuente: https://blockchain.info/es/charts/n-transactions

3.5. SEGURIDAD

Tal y como se comenta en la página web "guiabitcoin.com: ¿Cómo funciona la seguridad de bitcoin?"[13], si se piensa en términos matemáticos, la seguridad del Bitcoin debe ser pensada como infranqueable y es allí en donde se encuentra el secreto de la seguridad de esta plataforma. En otras palabras, no sería posible que todas las personas en el mundo que usan esta criptomoneda, confiasen en ella.

Por otro lado, en lo que respecta a los desarrollos a futuro, en caso que se construyan algoritmos de cifrado y hash más viables y seguros, el Bitcoin se actualizaría para utilizar esta clase de tecnología tan novedoso, para que de tal modo, su seguridad fuese lo más óptima posible.

Los principales agujeros de seguridad están directamente relacionados con los usuarios y suelen consistir en la divulgación de las claves privadas y contraseñas de cifrado. La divulgación de tal información puede deberse a descuidos en su custodia (pérdidas, anotaciones en lugares indebidos, transmisiones por canales inadecuados…) y a actos intencionados (robos, espionaje, sabotaje…).

Circunstancias que no suponen ninguna novedad en nuestra sociedad y que no están provocadas ni propiciadas por la tecnología utilizada en el sistema. Este riesgo no es realmente nuevo, puesto que las prácticas para proteger y asegurar los Bitcoins son las mismas que usan para proteger otros datos personales.

[13] Consultado el 01/07/2017 en http://guiabitcoin.com/funciona-la-seguridad-bitcoin/

Numerosas web ofrecen recomendaciones para garantizar la seguridad. Ejemplo de ello la web "queesbitcoin.info: ¿Es bitcoin seguro?"[14], muestra las siguientes recomendaciones:

- No compartir ni mostrar la clave privada, ni perderla u olvidarla. Casi siempre la clave privada es guardada y protegida por la misma aplicación de Bitcoin que se utilice. De todos modos también se puede exportar para usarla en otra aplicación. En caso que sea necesario, es mejor optar por escribirla en un trozo de papel.

- Función de cifrado y sistema de recuperación de las aplicaciones Bitcoin. La plataforma de Bitcoin permite activar esta función para que la clave privada esté protegida.

- Usar contraseña largas (con varios tipos de caracteres y que no contengan datos personales).

- Mantener el ordenador limpio de virus, troyanos y similares. Mantener el ordenador limpio en todo momento para no estar expuesto de manera innecesaria.

- Evitar carteras en línea poco confiables. Verificar que una cartera en línea sea fiable. Consultar en comentarios o en sitios web especializados para salir de dudas.

- Hacer copias de seguridad de todos los elementos importantes

[14] Consultado el 01/07/2017 en https://www.queesbitcoin.info/como-utilizar-bitcoin/seguridad/

CAPÍTULO 4

USO DEL BITCOIN

4.1. PERFILES DE USUARIOS BITCOIN.

Hay muchas suposiciones acerca de los usuarios Bitcoin: que son bichos raros, fantasiosos, criminales, idealistas, etc. Yelowitz y Wilson (2015), realizan un estudio de los usuarios de Bitcoin mediante el análisis de las tendencias de Google, metodología empleada por Hall y Kreuger (2016) en su estudio sobre Uber, que consiste en evaluar las consultas realizadas, como variable proxy de la participación activa.

Yelowitz y Wilson identifican cuatro tipos de usuarios Bitcoin: los entusiastas de la programación informática, los inversores especulativos, los partidarios del libre comercio y los criminales (2015, pag. 1030).

Esto, en gran medida, como comenta Ennis (2016) "para coindesk.com: The four types of Bitcoin users" [15], se ajusta al perfil "esperado" de los usuarios Bitcoin y concuerda con los resultados obtenidos en una encuesta del 2013 hecha a mil usuarios, mediante la cual se conoció que "el usuario promedio es de 32 años de edad, de sexo masculino y libertario".

Desde la perspectiva de estos cuatro tipos de usuarios, los principales motivos para la adhesión a Bitcoin son:

- Para los informáticos, las recompensas por la minería.
- Para los especuladores, la volatilidad.
- Para los defensores de las libertades, la falta de regulación percibida.
- Para los delincuentes, el anonimato

4.2. "MINING POOLS"

Tal y como se hace mención anteriormente, la práctica de la minería para conseguir monedas Bitcoin es cada vez más complicada. El tiempo aproximado para generar un bloque es de 10 minutos, tiempo que se controla mediante la dificultad del problema que tienen que resolver los mineros para encontrar la solución de dicho bloque. La dificultad aumenta en función del poder computacional de todos los mineros. Así cuantas más personas y con mejores equipos estén involucradas en la minería, mayor será la dificultad del problema y, por lo tanto, obtener la ansiada recompensa. Tal y como se aprecia en la Figura 15, la dificultad de encontrar un nuevo bloque cada vez es mayor como consecuencia de la gran cantidad de minero que existen a 26/06/2017.

De ello surgen los "mining pools" o "agrupación de mineros". Según Tuwiner (2017) para el portal de "bitcoinworldwide.com: bitcoin mining pool"[16] son definidos como grupos de mineros cooperadores que acuerdan compartir ganancias de bloques en proporción al poder de hash de minería contribuido.

[15] Consultado el 05/07/2017 en https://www.coindesk.com/four-types-bitcoin-users/

[16]Consultado el 15/07/2017 en https://www.buybitcoinworldwide.com/mining/pools/

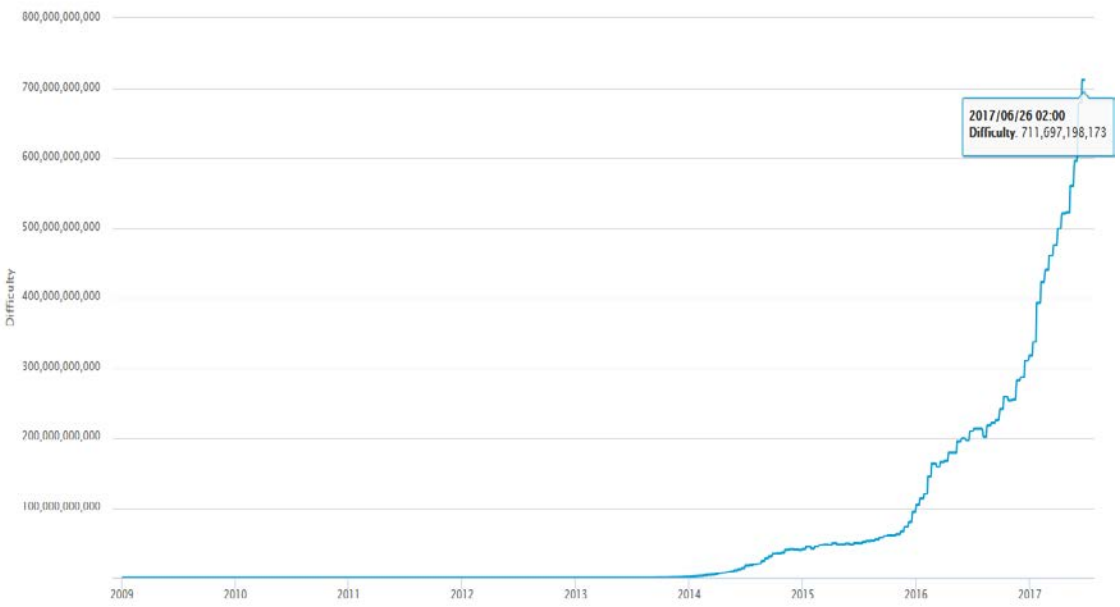

Figura 15. Dificultad para generar un nuevo bloque.
Fuente: https://blockchain.info/es/charts/difficulty

Los “pools” tal y como explica Alonso (2015, pag 345), agrupan todo su poder computacional y actúan como si fueran un único minero, de tal manera que, la probabilidad de resolver el problema es muy elevada.

En la Figura 16 se muestran a 26 de Junio de 2017 las organizaciones más grandes que practican “pools mining”. Aunque dada su volatilidad, en los días siguientes podría cambiar.

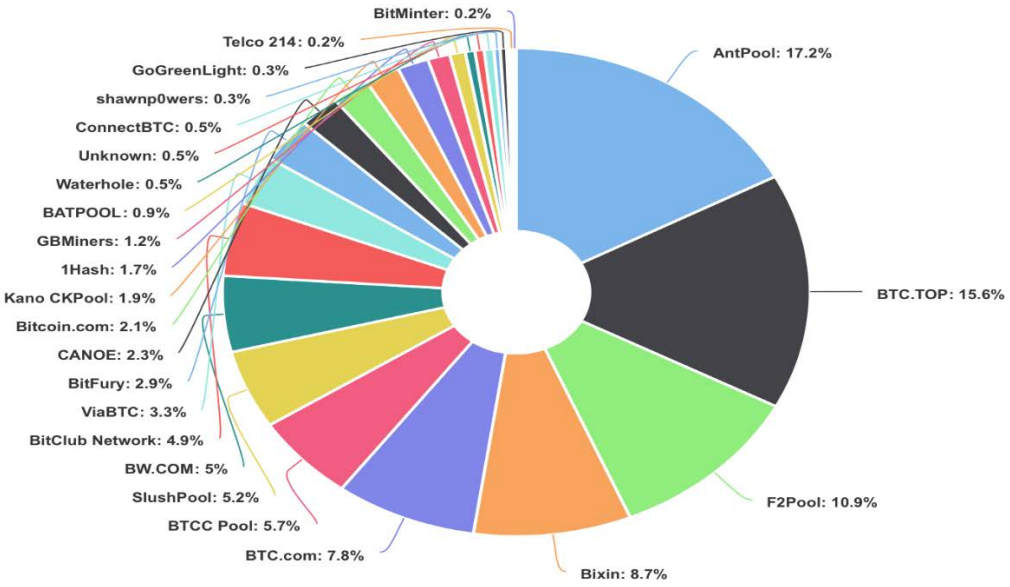

Figura 16. Distribución de las compañías más grandes en la minería Bitcoin.
Fuente: https://blockchain.info/es/pools

Las principales características de las siete "mining pools" que dominan el mercado del bitcoin a dia de hoy según el artículo publicado por Hernández (2015) para "criptonoticias.com: las 16 empresas más grandes en la minería bitcoin"[17] son:

- AntPool; grupo dirigido por Bitmain, el mayor proveedor de hardware para la minería Bitcoin y otros servicios relacionados con sede en Pekín. El objetivo de Bitman con este grupo es contribuir con la descentralización y la solidez de la red Bitcoin. Además, la mayor parte de la capacidad de procesamiento está en manos de los usuarios. Este grupo representa el 56% de todos los mineros Bitcoin y además pretende ser el mayor servicio de minería en la nube del mundo. Domina el 17,2% del mercado.

- BTC.Top; tal y como publica tuwiner (2017) en su artículo para "bitcoinworldwide.com: Bitcoin Mining Pools"[18], son pocos los datos que se conocen de ella al ser una compañía privada y debido al poco tiempo que lleva en funcionamiento.

  Actualmente se ha convertido en uno de los líderes con un poder tecnológico global en el mundo Bitcoin. Reúne el 15,6% del mercado.

- F2Pool, también conocido como Discusfish por su logotipo, es un grupo chino dirigido por Wang Chun y Mao Shihang que abrió sus puertas el 5 de mayo del 2013. De acuerdo con la web "CoinDesk.com", constituye aproximadamente el 25% de la red Bitcoin y el 30% de la red litecoin. En julio del 2015 generó la mayor transacción jamás registrada con el fin de aclarar un ataque de spam lanzado a la red. Además, el 100% de su capacidad de procesamiento proviene de los usuarios. Controla el 10,9% del mercado.

- Bixin, según el artículo publicado por Shadowargel (2017) para el portal de "diariobitcoin.com: HaoBTC anuncia suspensión de su servicio tras medidas del banco popular de china"[19], también es conocida como HaoBTC, y es una de las pequeñas plataformas que opera en el territorio del país asiático. Fue lanzada oficialmente en el mes de abril de 2016 registrando un volumen superior a los 3.000 bitcoins en operaciones comerciales durante su primera semana de lanzamiento.

  El 15 de febrero de 2017, debido a la escasa rentabilidad que tenía el servicio de intercambio para sus usuarios tras la incorporación de las nuevas medidas emitidas por el Banco Central del país asiático, le llevaron al cierren.

  Al dejar de ser rentable para los usuarios, HaoBTC comenzó a registrar una disminución en sus volúmenes de operaciones. En vista de dicho panorama, los directivos decidieron anunciar el cese de operaciones para no generar mayores incomodidades a los clientes afectados por las medidas. A día de hoy, es difícil conocer los efectos que tendrá en un futuro esta decisión, debido a la escasa información que hay sobre este tema. Domina el 8,7% del mercado.

[17] Consultado el 02/07/2017 en https://criptonoticias.com/mineria/las-16-empresas-mas-grandes-en-la-mineria-bitcoin/#axzz4lQm4TK53

[18] Consultado el 15/07/2017 en https://www.buybitcoinworldwide.com/mining/pools/

[19] Consultado el 03/07/2017 en http://www.diariobitcoin.com/index.php/2017/02/14/haobtc-anuncia-suspension-de-su-servicio-tras-medidas-del-banco-popular-de-china/

- BTC.com; según la web "www.territoriobitcoin.com (2017): Pool de minería bitcoin BTC.com anuncia nuevo modo para incrementar ingresos de los mineros"[20], es una empresa de rápido crecimiento y promotor líder universal en datos de bitcoin, Pool de minería y wallet multiplataforma. Está comprometida con la innovación continua, la cual a través de esta tiene como objetivo, reducir aún más el umbral de entrada en la industria de la minería Bitcoin y promover la descentralización. El equipo de BTC.com continua ofreciendo a sus usuarios una mejor experiencia Bitcoin. Ejemplo de ello es el lanzamiento que hizo en el mes de marzo del nuevo modo de asentamiento para los mineros denominado "Full pay per share" (FPPS) o lo que es lo mismo "Pago completo por acción". De esta manera los ingresos de los mineros han subido hasta en un 9% en ciertos niveles de las tarifas por transacción comparado con el modelo tradicional. Plataforma que reúne el 7,8% del mercado.

- BTC China Pool comenzó a funcionar a finales del 2014, pero ha crecido considerablemente a pesar del poco tiempo que la empresa lleva en funcionamiento. Este grupo es dirigido por BTC China, una de las mayores casas de cambio bitcoin de China fundada en el 2011 y dirigida actualmente por Bobby Lee. Controla el 5,7% del mercado.

- Slush, conocido formalmente como Bitcoin Pooled Mining, es el grupo de minería público más antiguo del mundo. Situada en la República Checa. Fue fundado en el 2010 por SatoshiLabs con el objetivo de introducir nuevas características y tecnologías que hagan la minería accesible a los nuevos mineros manteniéndola atractiva para sus actuales usuarios avanzados. Desde sus inicios en diciembre del 2010 este grupo lleva más de 939.000 BTC minados. Reúne el 5,2% del mercado.

4.3. EVOLUCIÓN Y ACEPTACIÓN

Como expresa Sandoval (2017) en su artículo para "cointelegraph.es: Las predicciones para bitcoin en el 2017"[21], a inicios del año pasado, la criptomoneda ha tenido un crecimiento importante en su valor histórico y cerró el 2016 como el activo con mayor rendimiento (120%), pero no queda ahí la cosa, tal y como se publica en el blog de "caixabank.es (2017): El bitcoin hace historia: supera el valor del oro"[22], durante el mes de marzo de 2017. El bitcoin fue protagonista de otro hito histórico nunca visto: superar el valor de una onza de oro, e incluso hasta el de superar los dos mil dólares en el mes de mayo, Figura 17. Si se toma como referencia el acumulado de los 12 últimos meses, las cifras son todavía más espectaculares: un incremento de casi un 400 %.

El hecho de superar el valor de una onza de oro se debe a la coincidencia de dos factores claves: la caída del valor del oro y la subida del valor del bitcoin.

Así, mientras el valor del bitcoin se situaba en 1.286,35 dólares según la web "CoinDesk.com", el del oro se quedaba en 1.227,37 dólares según "bloomberg.com".

Este hecho pone en evidencia una vez más que el valor del bitcoin sigue en ascenso imparable.

[20] Consultado el 03//07/2017 en https://www.territoriobitcoin.com/pool-de-mineria-bitcoin-btc-com-anuncia-nuevo-modo-para-incrementar-ingresos-de-los-mineros/

[21] Consultado el 04/07/2017 en https://cointelegraph.es/news/predicciones-bitcoin-2017/es

[22] Consultado el 04/07/2017 en https://blog.caixabank.es/2017/06/el-bitcoin-hace-historia-supera-el-valor-del-oro.html

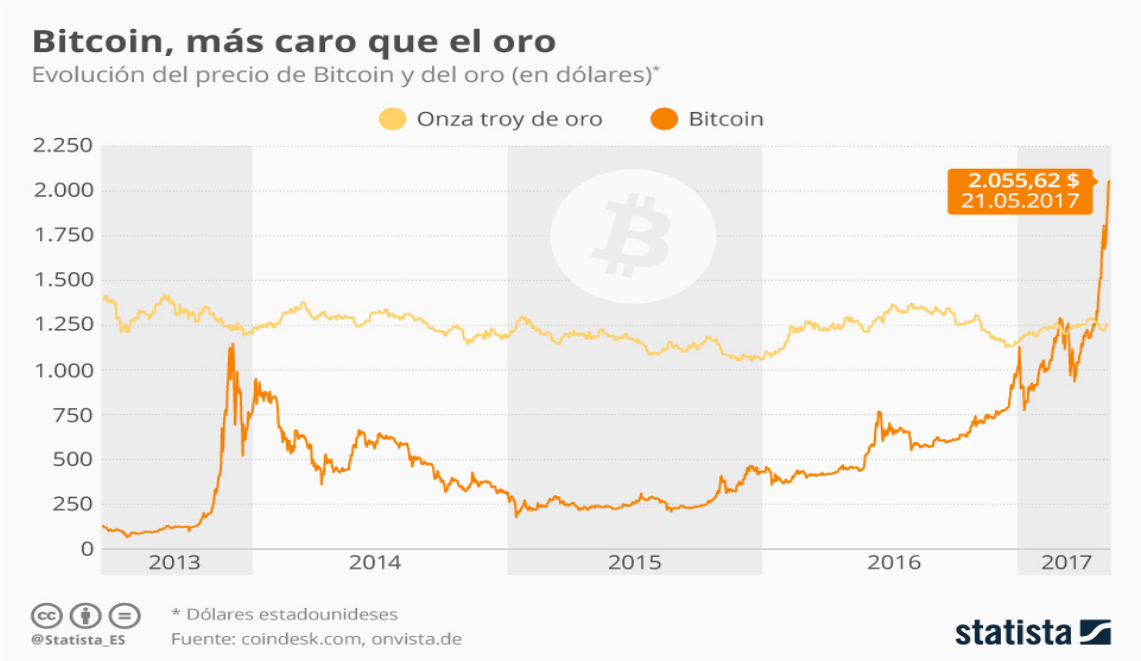

Figura 17. Evolución del precio Bitcoin y del oro
Fuente: coindesk.com

Sin embargo, tal y como Sandoval (2017) comenta, la volatilidad que presenta Bitcoin es muy alta, al cierre del año 2016 la moneda se situaba con un valor de 970$ según "coinDesk.com", a fecha de 26 de junio de 2017 el panorama se presenta un poco diferente puesto que, venimos de ver cómo bitcoin alcanzaba un nuevo máximo histórico el 11 de junio de 2017 con un valor de 3018,54$ según "CoinDesk.com" y caía de forma estrepitosa unos 300$, todo esto en cuestión de solo horas. A 26 de junio del 2017 el precio del Bitcoin se situó en 2436$, tal y como se muestra en la Figura 18 según "blockchain.com", y en donde además, se aprecia la evolución que ha tenido la moneda desde su lanzamiento.

Figura 18. Precio del Bitcoin en dólares.
Fuente: https://blockchain.info/es/charts/market-price

Además, se dan diferencias del precio del Bitcoin según la casa de cambio que se trate. Las características y diferencias de cada una de ellas, provocan que la tasa de cambio no presente un valor único, si no que sea una franja, más o menos acotada, en la que se mueve el valor del Bitcoin como se observa en la Figura 19. En determinados días, existe alguna plataforma en la que se da un valor de cambio anormalmente alto o bajo con respecto a los valores de las demás.
Tal y como expresa Rosembuj (2015), dichas situaciones pueden provocar un efecto especulativo brutal, dado que, el valor de una plataforma se multiplica o se divide por 3 o por 4 respecto al de las demás.

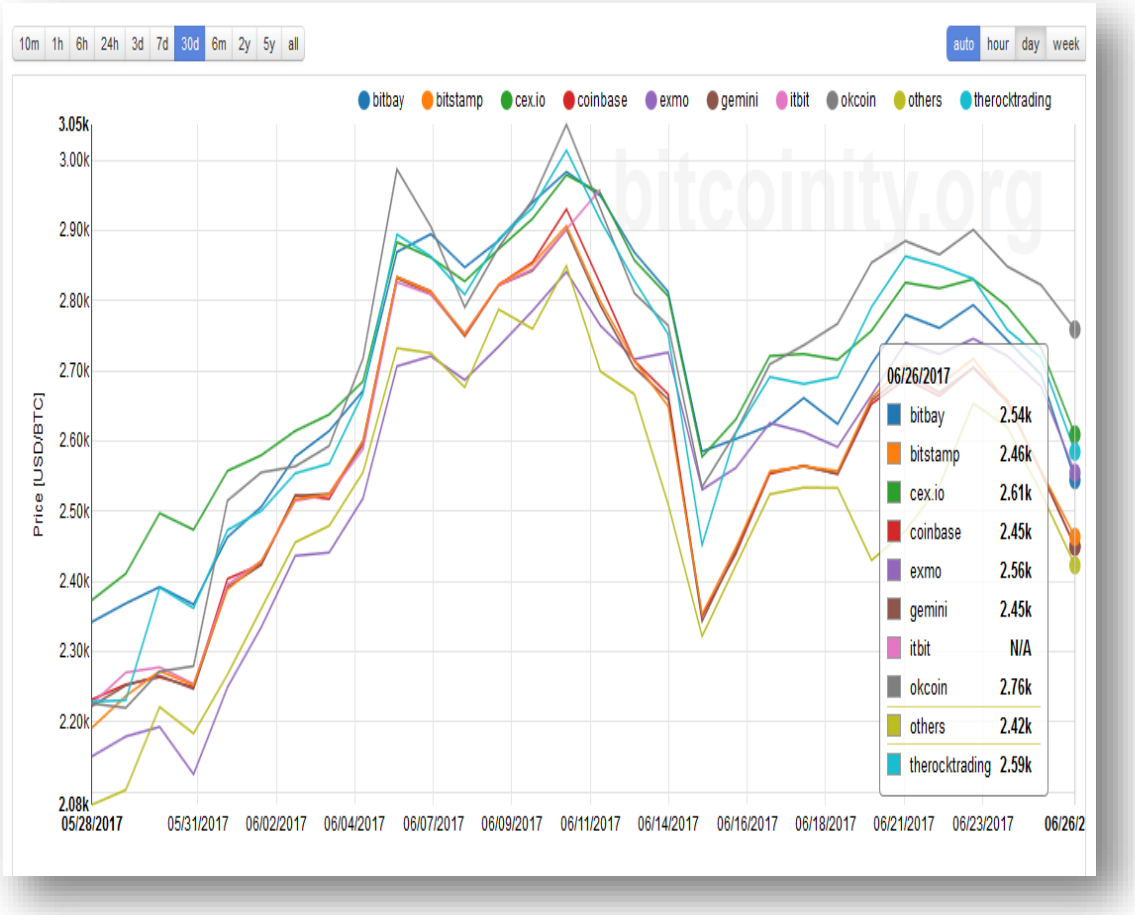

Figura 19. Precio del Bitcoin en dólar en función de las distintas casas de cambio
Fuente: http://data.bitcoinity.org/markets/price/30d/USD?c=e&t=l

A pesar de la volatilidad que hoy impera al bitcoin, las predicciones para el 2017 siguen siendo positivas en los mercados.

El número de empresas y pequeños negocios que aceptan bitcoin como medio de pago se encuentra en constante aumento. Su uso seguirá siendo dominado por el intercambio comercial, como moneda para el cambio y contratación de servicios, y poco a poco también para la venta y el comercio electrónico, sin embargo siempre de manera bastante restringida por parte de un nicho relativamente pequeño de la población.

En la Figura 20 se visualiza como en gran parte de América y de Europa la moneda es recibida en distintos establecimientos.

Figura 20. Uso del Bitcoin en el mundo
Fuente: mercadobitcoin.com

Siguiendo con Rosembuj (2015), en una economía como la europea, esta moneda está creando su mercado a pasos agigantados. Es así como en España está aumentando la adopción de Bitcoin y ya hay multitud de comercios que aceptan esta moneda como pago de sus productos o servicios en gran parte del territorio nacional, como se muestra en la Figura 21. La calle Serrano, de Madrid, pasó a llamarse la calle “bitcoin”, puesto que desde el 2014 muchos establecimientos ubicados allí reciben la moneda. Siguiendo con el blog de “caixabank.es (2017): El bitcoin hace historia: supera el valor del oro”, en el caso de España, se trata del cuarto país con más cajeros bitcoin del mundo: dispone de un total de 27**.**

Figura 21. Comercios que usan Bitcoin en España
Fuente: mercadobitcoin.com

El ranking de estados con más cajeros bitcoin instalados está encabezado por Estados Unidos y Canadá, con un total de 554 y 135 respectivamente. Así se observa en la Figura 22.

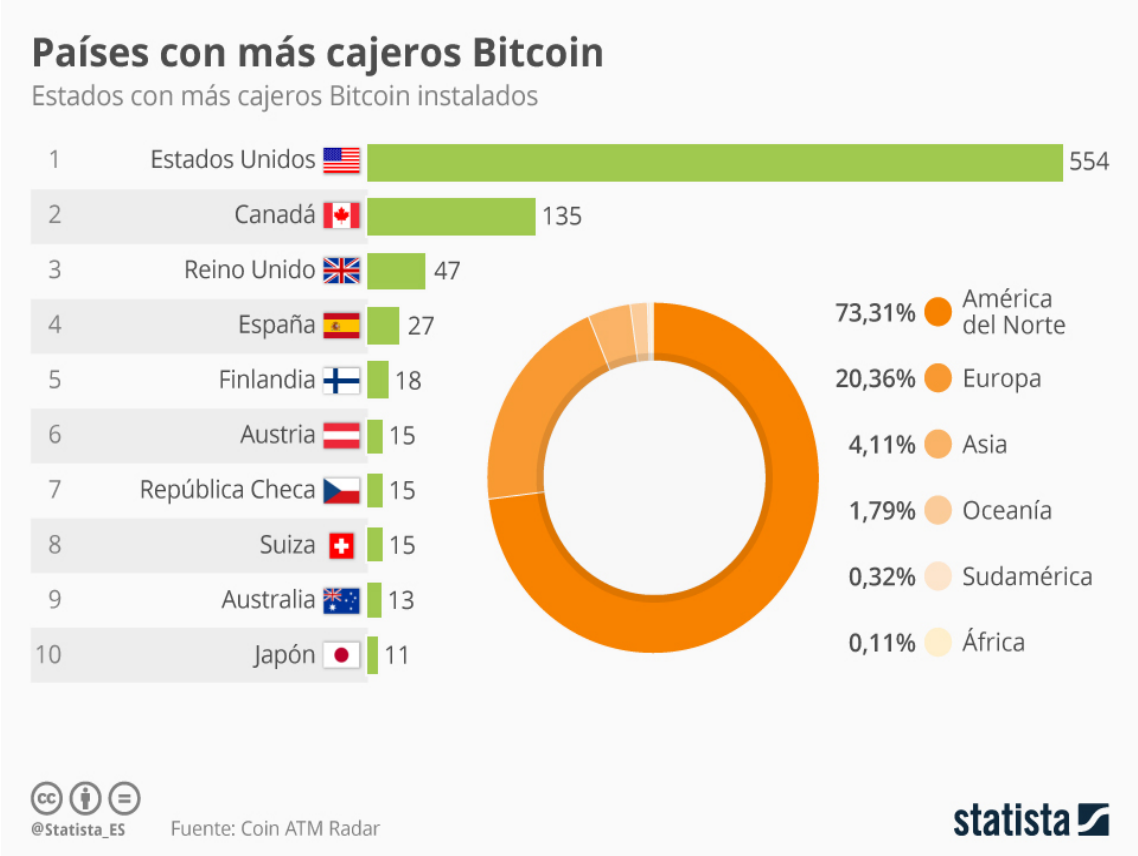

Figura 22. Países con más cajeros Bitcoin
Fuente: Coin ATM Radar

Pero no en todos los países la moneda es igualmente aceptada.

- En el caso de Colombia, según el artículo de "semana.com (2016): ¿El bitcoin es legal en Colombia?"[23], el Banco de la República, por medio de la Superintendencia Financiera, se pronunció en el 2014 sobre el tema del Bitcoin, estableciendo que el peso era el "único medio de pago de curso legal con poder liberatorio ilimitado".
  Alguna de las advertencias que se hace la Superintendencia es que las transacciones en las plataformas de bitcoin son anónimas, por lo que el uso de monedas virtuales se puede prestar para adelantar actividades ilícitas o fraudulentas, incluso para captaciones no autorizadas de recursos, lavado de dinero y financiación del terrorismo.
  Los compradores o vendedores de estas monedas virtuales se exponen a riesgos operativos, principalmente a que las billeteras digitales sean robadas (hackeadas), tal como ya ha ocurrido, y a que las transacciones no autorizadas o incorrectas no puedan ser reversadas.

[23] Consultado el 04/07/2017 en http://www.semana.com/economia/articulo/bitcoin-legalidad-de-la-divisa-en-colombia/475730

- Bangladesh; tal y como se expresa en el artículo publicado por Sandoval (2015) para "criptonoticias.com: top 10 de países que declaran a bitcoin prohibido"[24], el Banco Central de Bangladesh citó en un comunicado oficial la preocupación por la falta de "un sistema de pago central" que podría llevar a la gente a ser "perjudicada financieramente" con bitcoin. En Bangladesh su uso está prohibido, haciendo mención de que el comercio en bitcoin y otras monedas digitales podría conducir a una pena de hasta 12 años de prisión.

- Bolivia; según el Banco Central de Bolivia:[25]
  "Es ilegal utilizar cualquier moneda que no esté emitida y controlada por un gobierno o una entidad autorizada "

- Ecuador; siguiendo con Sandoval (2015), la prohibición por el estado de Ecuador tiene más sentido que cualquier otra prohibición, ya que en ese país están construyendo un sistema de dinero electrónico nacional, por lo que se siente la necesidad de proteger su nueva moneda de algo claramente superior. Una moneda descentralizada de producción finita que no puede ser manipulada por los gobiernos o bancos podría atenuar las luces en su nuevo programa a los ojos del público, que no ofrece ninguno de esos beneficios.

- China[26], a pesar de ser el país con mayor número de transacciones de bitcoin, no permite el uso de la criptomoneda en los bancos y sus empleados, sin embargo, cambiar o minar bitcoin no es ilegal para usuarios comunes.

- Rusia. Como comenta Datica (2017), las autoridades esperan reconocer a Bitcoin y otras criptomonedas en 2018, procurando implementar reglas contra las transferencias ilegales de dinero.[27]

4.4. EL BITCOIN EN ESPAÑA

Según el artículo publicado por Gomá (2014) para el blog hayderecho.com: ¿se puede constituir una sociedad con Bitcoin?, la definición que en España se tiene de bitcoin según lo establecido en su ordenamiento jurídico, que pueda resultar afín, es:[28]

> "Un Bitcoin es un bien patrimonial inmaterial, documento electrónico, objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada "Bitcoin", que permite ser utilizada como contraprestación en transacciones de todo tipo. Dichas unidades de cuenta son irrepetibles, no son susceptibles de copia y no necesitan intermediarios para su uso y disposición"

[24] consultado el 04/07/2017 en https://criptonoticias.com/colecciones/top-10-paises-bitcoin-prohibido/#axzz4kudY2GdW

[25] Consultado el 26/6/2017 en http://elperiodico-digital.com/2017/04/17/banco-central-advierte-que-esta-prohibido-uso-de-monedas-virtuales-como-el-bitcoin/

[26] Consultado el 04/07/2017 en http://www.diariobitcoin.com/index.php/2015/05/27/10-paises-en-los-que-bitcoin-esta-prohibido/

[27] Consultado el 26/06/2017 en http://www.diariobitcoin.com/index.php/2017/04/11/rusia-anuncia-que-reconocera-oficialmente-a-bitcoin/

[28] Consultado el 29/06/2017 en http://hayderecho.com/2014/06/09/se-puede-constituir-una-sociedad-con-bitcoin

Dicho lo anterior también cabe destacar cómo afecta el Bitcoin ante la aplicación, de leyes tributarias como puede ser el Impuesto del Valor Añadido, o cualquier otro tributo.

Tal y como comenta Gómez (2015), el Ministerio de Hacienda de España declara oficialmente:[29]

> "Bitcoin y las criptomonedas siempre han estado exentas de IVA en España. La decisión se basa en la interpretación de la directiva europea (2006/112/CE) que regula el sistema común del impuesto sobre el valor añadido y es vinculante."

Se ha determinado que debe ser incluido dentro de la categoría de "Otros Efectos Comerciales" por lo que la transacción quedará sujeta al impuesto, pero exenta del mismo.

Por todo ello, en caso de tener la residencia española, se podrán comprar Bitcoins en la Unión Europea y aunque en el país de origen tribute, como el caso de Estonia y Polonia, se le aplicará el impuesto español, el cual estará exento.

A día de hoy, el interés por el bitcoin en España no ha dejado de aumentar. Las búsquedas sobre el tema de los bitcoins crecen a nivel nacional según Google Trends. Se estima que el número de consultas relevantes sobre el tema (bitcoins, criptomonedas y blockchain) ha alcanzado el nivel máximo en 2017.

Las ciudades en donde más se refleja la búsqueda de al menos el significado de Bitcoin desde su aparición son Barcelona, Málaga, la Coruña, Valencia, Zaragoza, Sevilla y Madrid, tal y como se puede apreciar en la Figura 23. Estas ciudades han mostrado un mayor interés en la innovación e inclusión de los bitcoins en sus negocios y ahorros.

En cuanto a las comunidades autónomas que más interés han mostrado en la búsqueda de bitcoins son las Islas Baleares, Canarias, Cataluña, Principiado de Asturias y Comunidad Valenciana, tal y como se refleja en la Figura 24.

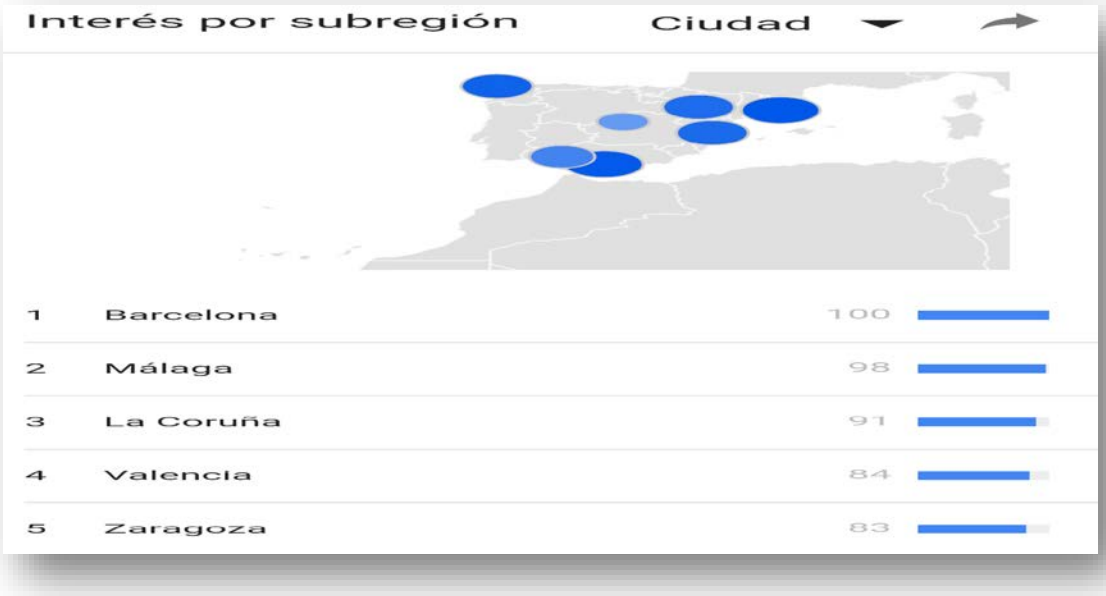

Figura 23. Interés del Bitcoin en España por ciudades
Fuente: https://trends.google.es/trends/explore?date=all&geo=ES&q=bitcoin

[29] Consultado el 30/06/2017 en http://lawandbitcoin.com/bitcoin-exento-de-iva-en-espana/

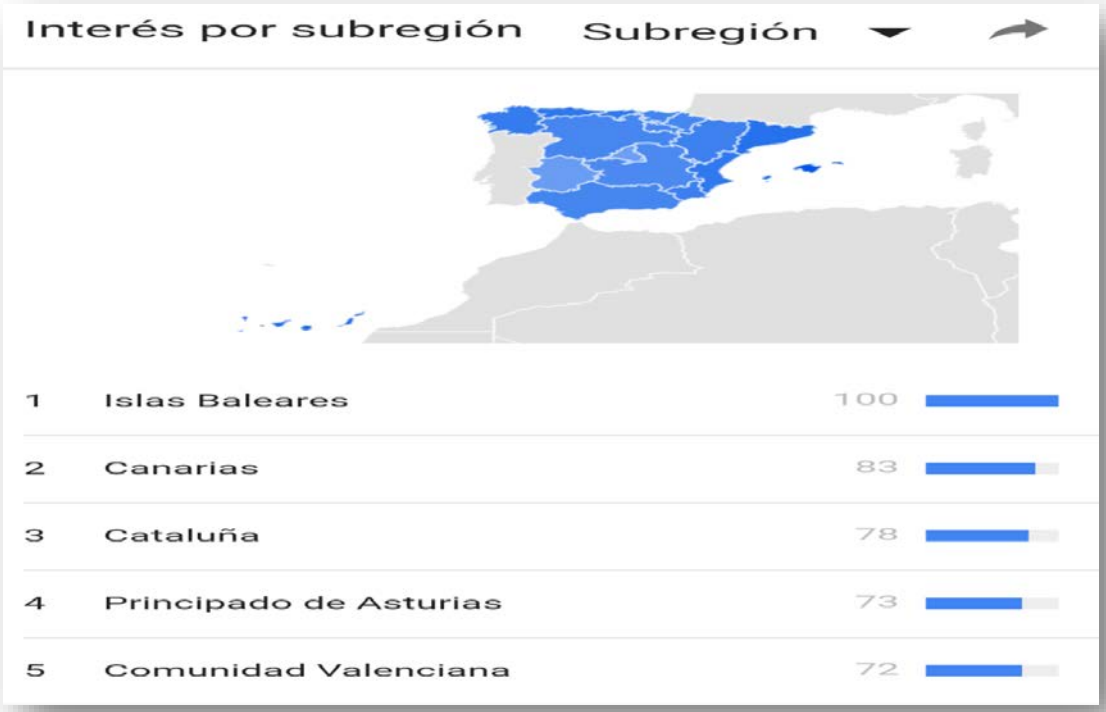

Figura 24. Interés del Bitcoin por comunidades
Fuente: https://trends.google.es/trends/explore?date=all&geo=ES&q=bitcoin

Figura 25. Interés del Bitcoin en España
Fuente: https://trends.google.es/trends/explore?date=all&geo=ES&q=bitcoin

4.5. ALTCOINS O MONEDAS ALTERNATIVAS

Según Antonopoulos (2014, pag 78), las altcoins se definen como una construcción simplificada de las palabras “alternative” y “coins”. Podría traducirse, por tanto literalmente como “monedas alternativas”. El término Altcoins se refiere a criptomonedas que derivan del código fuente de Bitcoin también conocidas como “Forks”. Hay gran variedad de Altcoins, pero todas tienen en común que son implementaciones de monedas que surgen a partir del diseño informático y de la lógica de funcionamiento del Bitcoin. Existen más de 900 monedas virtuales y toda la relación exhaustiva de cada una de ella puede ser encontrada en lo que se llama la biblia de las criptomonedas “coinmarketcap.com”.

Las Altcoins que se van creando en el mercado de las criptomonedas existen de todas las variantes. Muchas de ellas le han dado una mala reputación a la comunidad de las criptomonedas porque han sido esquemas que se han desarrollado para atraer inversores a la nueva moneda organizados con una potente campaña de marketing para inflar el precio y cuando se han colocado suficientes de la misma, abandonan el proyecto. De hecho hay personas que se han especializado en ese mercado y se han hecho conocidos por organizar este tipo de fraudes en cadena.

Al mismo tiempo, algunas de esas Altcoins han sido increíblemente rentables para aquellas personas que decidieron arriesgarse desde muy pronto o tenían los contactos adecuados para participar.

A continuación se detallan en la Figura 26 las que tienen una mayor capitalización de mercado a 27 de junio 2017. Aunque dada su volatilidad, en los próximos días podría cambiar.

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$43,397,275,463	$2644.44	16,410,762 BTC	$974,201,000	0.10%	
2	Ethereum	$29,310,606,655	$315.90	92,783,859 ETH	$810,161,000	-4.91%	
3	Ripple	$11,670,066,257	$0.304770	38,291,387,790 XRP *	$138,996,000	-1.76%	
4	Litecoin	$2,351,039,814	$45.47	51,710,982 LTC	$342,558,000	0.94%	
5	Ethereum Classic	$2,098,371,530	$22.58	92,947,826 ETC	$413,685,000	10.13%	
6	NEM	$1,651,824,000	$0.183536	8,999,999,999 XEM *	$4,822,590	-1.36%	
7	IOTA	$1,358,173,000	$0.488634	2,779,530,283 MIOTA *	$6,079,110	-5.01%	
8	Dash	$1,325,650,119	$179.53	7,384,086 DASH	$34,561,400	-1.77%	

Figura 26. Clasificación de las principales altcoins en función de su capitalización de mercado
Fuente: coinmarketcap.com

Ethereum

Según el artículo publicado por Camero (2016) para "diariobitcoin.com: Las criptomonedas más populares en el mercado"[30], ha sido la más publicitada de las tecnologías de Bitcoin 2.0. Últimamente, su valor ha subido, tal vez gracias a la cuestión que rodea el límite del tamaño del bloque en bitcoin. Por los momentos, se mantiene como la primera criptomoneda alternativa, por detrás de bitcoin. La divisa consiguió casi 20 millones de dólares, con el fin de asegurar que el proyecto despegara. Muchos creen que Ethereum puede conseguir lo que bitcoin no.

Ripple

Siguiendo con Camero (2016) para "diariobitcoin.com: Las criptomonedas más populares en el mercado", es diferente que Litecoin *y* Bitcoin. Para empezar, es una moneda "pre-minada", que no quiere decir otra cosa que los desarrolladores de la misma han decidido repartir un porcentaje de dicha moneda o toda entre unas cuantas personas o ellos mismos. Lo que significa que no es una buena opción para ningún inversor, por no mencionar que ha perdido más de su 90% de capital de mercado en los dos años pasados.

Ripple se considera a sí mismo como "un sistema de liquidación bruta a tiempo real", y tiene funciones como un mercado cambiario y una red de envío de remesas operada por una compañía privada del mismo nombre. El Protocolo de Ripple es de código abierto. Podría ser que Ripple esté sirviendo de inspiración para muchas instituciones financieras privadas mirando hacia bitcoin.

Litecoin

Siguiendo con el artículo de la web "oroyfinanzas.com (2014): ¿Qué son las altcoins?", Litecoin se caracteriza por tener un tiempo de confirmación de sus bloques inferior al que tiene Bitcoin (2,5 minutos, en lugar de los 10 minutos de bitcoin) y por utilizar otro algoritmo de minado. Existe un límite total de 84 millones de monedas. Fue creada por Charlie Lee en 2011. A mediados de 2014, tenía una capitalización de mercado de aproximadamente 160 millones de dólares.

Ethereum Classic

Tal y como se expresa en el artículo publicado por Pérez (2017) en la web de "criptonoticias.com: Firma de inversión estadounidense planea introducir Ethereum Classic en el mercado de valores"[31], esta BlockChain es una bifurcación de Ethereum. Entró en funcionamiento como resultado de la hard-fork DAO el año pasado, luego de que fueran sustraídos 60 millones de dólares a una de sus aplicaciones descentralizadas. Muchos usuarios migraron al Ethereum actualizado, pero otros decidieron quedarse en la versión tradicional a pesar de todo. A día de hoy, esta blockchain está tomando un rumbo muy distinto al de su hermana más joven.

Nem

Inicialmente desarrollado e introducido en Japón por Makoto Takemiya. Según explica Young (2017) en su artículo para "cryptocoinsnews.com". La participación de Takemiya en algunos de los proyectos y consorcios de bloques más grandes y prominentes, así

[30] Consultado el 06/07/2017 en http://www.diariobitcoin.com/index.php/2016/02/24/las-criptomonedas-mas-populares-en-el-mercado/

[31] Consultado el 07/07/2017 en https://criptonoticias.com/mercados/firma-inversion-estadounidense-introducir-ethereum-classic-mercado-valores/#axzz4lrHaBR1J

como la legalización del bitcoin por parte del gobierno japonés, dio lugar a un aumento del interés por NEM. El factor más importante que ha permitido a NEM transformarse en uno de los altcoins más populares en Japón es su equipo de desarrollo y compañía compuesta de fundadores y talentos japoneses.

Iota

Tal y como comenta Molina (2017) en “cointelegraph.es: Las criptomonedas más prometedoras de 2017”[32], es un novedoso token para microtransacciones optimizado para el Internet-of-Things (Internet de las cosas – IoT). A diferencia de los blockchains complejos y pesados de Bitcoin y similares, que fueron diseñados con otros fines en mente, Iota se he creado para ser lo más ligera posible, de ahí el nombre de "Iota" con énfasis en la parte 'IOT'. A través de Iota, es posible transferir dinero sin ninguna comisión, incluso micropagos. Su proyecto, que sigue en fase Beta, ha estado envuelto de polémica por continuos retrasos y falta de comunicación del equipo con los inversores

Dash

Siguiendo con Molina (2017) para “cointelegraph.es: Las criptomonedas más prometedoras de 2017”, fue renombrada de Darkcoin a Dash (de la unión de digital cash) en marzo de 2015, la mayoría de la gente no sabe mucho sobre ella, pero está muy enfocada al uso diario. Actualmente pocas criptomonedas reúnen todas las ventajas que Dash puede ofrecer.

- Transacciones instantáneas confirmadas en cuestión de segundos.
- Útil para pagar en comercios minoristas. Especialmente con potencial para los países en desarrollo y menos bancarizados.
- No más cadenas de letras y números en las direcciones de monedero. Similar a la interfaz de Paypal y descentralizada.
- Transacciones privadas.

[32] Consultado el 07/07/2017 en https://cointelegraph.es/news/las-criptomonedas-m%C3%A1s-prometedoras-del-2017/es

CAPÍTULO 5

VENTAJAS, INCOVENIENTES Y PERSPECTIVAS DE FUTURO

5.1. VENTAJAS

Según González (2013, pag 39 y 40), las principales ventajas del Bitcoin son:

- Mayor privacidad, al eliminar la interferencia de terceros en las transacciones.
- Aumento decreciente y predecible de la masa monetaria, lo cual ayuda a preservar y probablemente a mejorar el poder adquisitivo de los usuarios.
- Menores, e incluso nulos, costes de transacción en la web, cuyos niveles actuales, por ejemplo a través de PayPal entorpecen el libre intercambio.
- Simplifica y acelera el pago de persona a persona, prescindiendo de intermediarios no deseados.
- Una dirección Bitcoin puede ser anónima, si así lo desea el usuario.
- Permite hacer transferencias a cualquier parte, ignorando barreras geográficas y políticas.
- Es transparente: aunque nadie está forzado a revelar su identidad, todas las transacciones quedan grabadas en un registro de libre acceso.
- Admite transacciones complejas (depósitos en custodias; seguros de depósitos; garantías; mediación, etc.) con un firme respaldo criptográfico para todo tipo de reglas y condiciones libremente acordadas por las partes.
- Nunca se detiene: no hay feriados ni fines de semana para las operaciones de bitcoins.
- Hace viables los micropagos a gran escala.
- Impide la congelación de fondos.
- Impide la reversión involuntaria de pagos.
- Impide la restricción arbitraria de bienes y servicios que pueden adquirirse.
- Permite la acumulación de fortunas enormes en un espacio ínfimo.
- Puede ocultarse fácil y gratuitamente sin tener que apelar a terceros para su resguardo y traslado.
- Se puede guardar en múltiples localizaciones simultáneamente.

- No requiere confianza en un tercero ni en un determinado sistema legal para preservar su valor.

- Facilita la protección contra el robo en todas sus formas impuesto inclusive: la tecnología en la que se basa el protocolo de Bitcoin es varias veces más segura que la empleada por los bancos y las tarjetas de crédito.

- No puede ser eliminado por ataques legales/informáticos, dada su naturaleza descentralizada.

- No puede falsificarse.

- Es fácil e instantáneamente reconocible.

- Es, a los fines prácticos, infinitamente divisible.

En resumen; siguiendo con González (2013), un sistema monetario como bitcoin, cuyas reglas premian la conducta mutuamente beneficiosa y desincentivan fuertemente la usurpación y el fraude, hace prácticamente imposible la falsificación, la inflación y el endeudamiento en nombre de otros. Pero bitcoin no tiene que ser un sistema perfecto; tan solo tiene que ser mejor que las alternativas monetarias hoy disponibles para llegar a ser ampliamente aceptado. En rigor, ningún aspecto de bitcoin puede ser considerado perfecto, pues está en su naturaleza evolucionar constantemente.

5.2. INCONVENIENTES

Actualmente son pocos los inconvenientes que se pueden encontrar del bitcoin, entre otras razones, porque está en pleno desarrollo, y debido a que el mecanismo que se está llevando a cabo para que se termine de dar a conocer es hacer hincapié en mostrar sus ventajas.

Según Alonso (2015, pag 425 - 430), los pocos inconvenientes que se pueden encontrar de Bitcoins son:

- Las transacciones son irreversibles. Es decir, si, por ejemplo, queremos enviarle a un amigo nuestro unos BTCs y nos equivocamos al escribir la dirección de su cuenta, los habremos perdido para siempre, sin la posibilidad de reclamar a nadie.

- El almacenamiento de la clave privada. Tenemos distintas formas de almacenarlas. Gracias a ella podemos gastarnos BTCs, por lo que debemos evitar, por todos los medios, su pérdida o robo.
  La mayoría de monederos para ordenador ofrecen la posibilidad de encriptar nuestra clave privada. En definitiva, transformarla de tal manera que sea incomprensible e indescifrable por cualquier persona que no tenga la contraseña por la que la hemos cifrado. De este modo, si un hacker entra en nuestro ordenador y nos roba el fichero donde está la clave privada, no podrá robar nuestros BTCs, ya que, si hemos elegido una buena contraseña (que no sea como 1234 o nuestro nombre), difícilmente podrá descifrar la clave. Así, si somos consciente de que nos han robado la clave privada (aunque sea encriptada), debemos crearnos una nueva dirección y transferir todos los fondos de la cuenta antigua a la nueva, eliminando la posibilidad del que hacker consiga hacerse con nuestros BTCs al descifrar la contraseña encriptada.

  Un inconveniente que surge al encriptar la clave privada es que tenemos que recordar la contraseña. Si la perdemos, no podremos ir al banco, como haríamos si olvidáramos la de nuestra tarjeta de crédito y solicitar una nueva. Sin embargo, han surgido empresas que ofrecen recuperar la contraseña haciendo uso de potentes

ordenadores que prueban millones de combinaciones en base a información que recuerda el cliente sobre la contraseña, como alguna de las palabras que contiene. Pese a lo anterior, estas empresas no ofrecen sus servicios a personas que no tengan ninguna idea de cómo era su contraseña, ya que, en este caso, es casi, por no decir imposible recuperarla, si, como hemos comentado, es mínimamente fuerte.

Tal y como hace mención Jesús Martín Alonso (2015) en el capítulo I para el libro: "Todo sobre Bitcoin". El hecho de que los BTCs aumenten su valor, atrae a los cibercriminales y cuyo único objetivo es enriquecerse. Estos crean virus que una vez dentro de un ordenador infectado, buscan cuentas en el sistema de archivos y las envían al cibercriminal. Así el número de virus relacionado con robo de esta moneda no para de crecer, de ahí la necesidad de tener la cuenta encriptada.

5.3. PERSPECTIVAS DE FUTURO

El incremento de bitcoin producido al final de 2016 y durante los primeros meses de 2017, no se espera que acabe aquí.

Según el artículo publicado por G.Lemos para el periódico: "la voz de Galicia: bitcoin, ¿refugio o burbuja?"[33], el incremento de bitcoin podría ser aún mayor, sobre todo si, como se espera, la nueva Administración Trump sigue con su ambicioso plan de inversión, lo que aceleraría la subida de tipos y dispararía el dólar, obligando a otras potencias a buscar alternativas monetarias.

Al igual que si Rusia y China se mueven para aceptar el bitcoin como una alternativa parcial al dólar y al sistema tradicional de banca, entonces podríamos ver que el bitcoin fácilmente triplique su valor durante el 2018.

En la siguiente Figura 27 se muestra la capitalización de mercado del bitcoin según la plataforma "BlockChain.com" el cual está en 39.989.166$. Así como en la Figura 28 se representa en función de las distintas casas de cambio.

[33] Consultado el 26/06/2017 en http://www.lavozdegalicia.es/noticia/mercados/2017/01/22/bitcoin-refugio-burbuja/0003_201701SM22P3992.htm

Figura 27. Capitalización de mercado del bitcoin
Fuente: https://blockchain.info/es/charts/market-cap

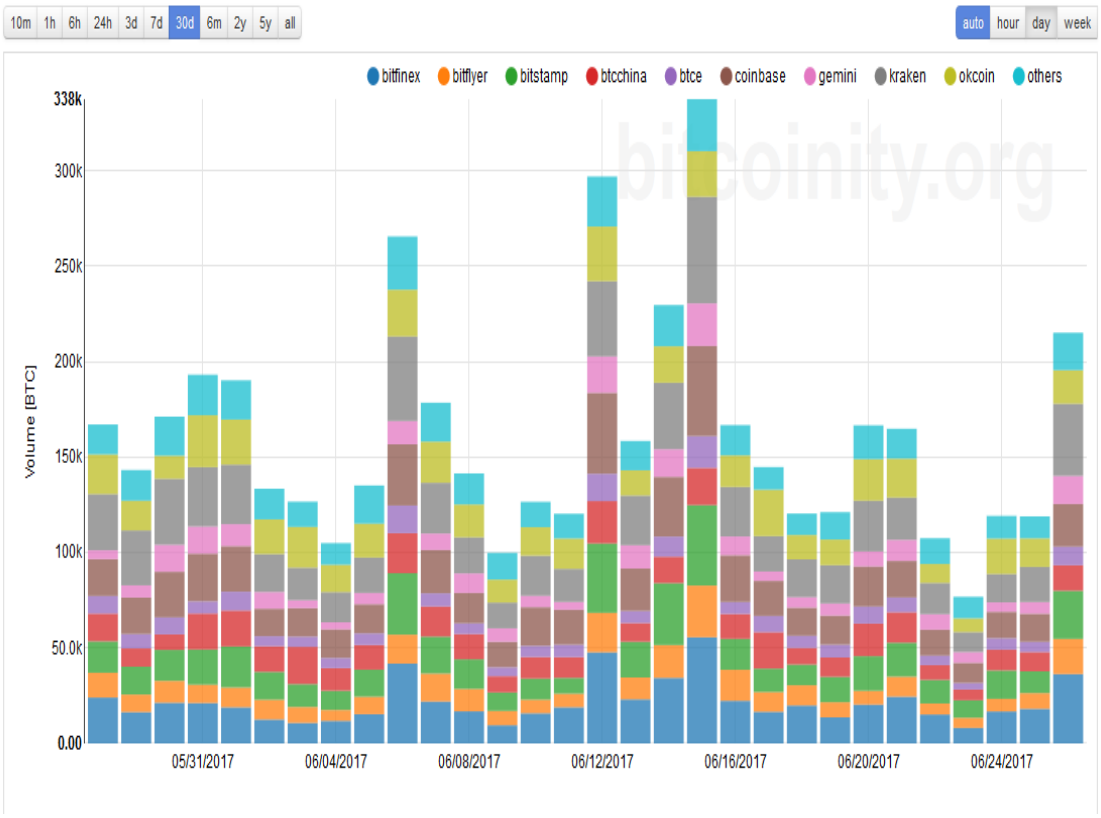

Figura 28. Capitalización de mercado en función de las distintas casas de cambio
Fuente: http://data.bitcoinity.org/markets/volume/30d?c=e&t=b

CAPÍTULO 6

CONCLUSIONES

6.1. CONCLUSIONES

Tal y como se ha podido observar a lo largo de todo el trabajo, el Bitcoin es una criptomoneda que, si bien se creó hace algunos años, su auge y "explosión" en el ámbito de la actividad económica ha sido reciente. Así desde agosto de 2008 hasta la actualidad, ha evolucionado hasta llegar a convertirse en una alternativa a las divisas emitidas por bancos centrales. Inicialmente, el cambio de un bitcoin se estableció por un valor de 0,3 centavos de dólar y llegó a superar el valor de una onza de oro e incluso a romper la barrera de los 3.000 dólares, algo que no podía imaginarse en sus comienzos.

Bitcoin cuenta con una compleja tecnología a sus espaldas que puede avalar el uso de ésta como moneda, ya que evita que se creen Bitcoins falsos, que se utilice el dinero más de una vez y además nos asegura un anonimato en las transacciones y sin comisiones. En resumen, desde el punto de vista técnico, el sistema Bitcoin ha conseguido un sistema de seguridad que ha generado la confianza para la extensión de su uso.

Desde la perspectiva económica y social, ha creado un espacio totalmente nuevo, donde es difícil pronosticar qué efectos tendrá y si será totalmente aceptado.

En este momento, y desde nuestra perspectiva, existen diversos obstáculos para que el bitcoin tenga un uso generalizado como moneda: la volatilidad, la confianza y la aceptación política.

Una de ellas es la volatilidad de precios que sufre debido a los movimientos especulativos. Esto le impide representar un depósito de valor seguro y formar una unidad de medida sin riesgo para los comercios.

Otro elemento a tener en cuenta es la confianza social en el bitcoin. La confianza, que en mi opinión creo que es la principal causa de su valor, puesto que, de perderse algún día, todo se vendría abajo.

En el momento en que desaparezca la confianza de los tenedores –y no tenedores- de Bitcoins en su funcionamiento, dejen de tener seguridad, no pueda ser utilizado como medio de pago porque ninguna institución lo reconoce o no hay ninguna facilidad al respecto... De producirse todo ello, supondría la caída drástica del Bitcoin y su posterior desaparición.

Además, aún en la actualidad, no todo el mundo utiliza internet para las transacciones bancarias por falta de confianza. Si no confían en este uso común y conocido, ¿cómo se van a fiar de algo nuevo, casi desconocido por muchos?

Otro de los problemas que se puede encontrar el Bitcoin para que siga evolucionando es su aceptación, ya que hay muchas personas que desconocen su existencia, o que no se fían de utilizarlo bien por no tener a alguien que lo regule, o por los problemas que ha tenido a lo largo de estos años con sus intermediarios financieros.

Si se quiere que el Bitcoin tenga éxito se debería empezar a admitir en todas las empresas como forma de pago, es decir, poder utilizarlo en un día a día en cualquier lugar, lo cual aumentaría la confianza al ser utilizada. Ahora bien, como la moneda presentase una evolución positiva, los Estados la verían como algo peligroso que podría

poner en desequilibrio sus estructuras político-económicas. Con lo cual, ellos podrían poner barreras a este desarrollo declarándola moneda ilegal para no perder el control de sus economías.

Por lo tanto, parece complicado que tenga éxito, no sólo porque sea difícil su aceptación en nuestra sociedad, sino que aunque tuviera éxito, los Estados no dejarían que llegara a tener una gran importancia.

Pero, a pesar de lo poco probable que es, que veamos al Bitcoin como moneda, como intento y como forma de ver cómo puede evolucionar una moneda en un futuro donde internet es cada vez más importante, me parece un experimento muy interesante.

Además, ¿quién sabe si las entidades financieras han visto en el Bitcoin, el futuro de una criptomoneda creada por ellas?

Bibliografía

Alonso, J. M. (2015): Un primer acercamiento al bitcoin. En Martín Fernández, J. (coord.) "Todo sobre Bitcoin: aspectos económicos, fiscales, contables y administrativos." (pp. 23-24). Francis Lefebvre, Madrid.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.".

Bitcoin, https://bitcoin.org/es/faq (Consultado: Junio - Julio 2017).

Bit2me, http://blog.bit2me.com/es/monederos-bitcoin-ligeros-para-ordenador (Consultado: 28/06/2017).

Bit2me, http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/ (Consultado: 28/06/2017).

Blockchain, https://blockchain.info/es (Consultado: Junio - Julio 2017).

Bloomberg, https://www.bloomberg.com/markets (Consultado: Junio – Julio 2017).

Coindesk, www.coindesk.com/price/ (Consultado: Junio – Julio 2017).

Caixa, La (2017): "El bitcoin hace historia: supera el valor del oro", 9 Junio 2017 https://blog.caixabank.es/2017/06/el-bitcoin-hace-historia-supera-el-valor-del-oro.html (Consultado: 04/07/2017).

Camero, G. (2016): "Las criptomonedas más populares en el mercado", 24 Febrero 2016. http://www.diariobitcoin.com/index.php/2016/02/24/las-criptomonedas-mas-populares-en-el-mercado (Consultado: 06/07/2017).

Capellá, M.P., Isern, P.A. Y Mut, M. (2014): "Sistemas de pago electrónicos", 3 Noviembre 2014. http://www.criptored.upm.es/crypt4you/temas/sistemaspago/leccion3/leccion03.html#apartado32 (Consultado: Junio – Julio 2017).

Criptonoticias.com (2016): "Usando la cartera de bitcoin mycelium", 15 Noviembre 2016. https://criptonoticias.com/tutoriales/tutorial-usando-cartera-bitcoins-mycelium/#axzz4lEiEJKo6 (Consultado: 28/06/2017).

Datica, D. (2017): "Rusia anuncia que reconocerá oficialmente a Bitcoin", 11 Abril 2017. http://www.diariobitcoin.com/index.php/2017/04/11/rusia-anuncia-que-reconocera-oficialmente-a-bitcoin/ (Consultado: 26/06/2017).

Diariobitcoin.com (2017): "10 países en los que bitcoin está prohibido", 27 Mayo 2017. http://www.diariobitcoin.com/index.php/2015/05/27/10-paises-en-los-que-bitcoin-esta-prohibido/ (Consultado: 04/07/2017).

Díaz, J. (2014): "Bitcoin: Funcionamiento y aspectos destacables", 10 Enero 2014. https://www.certsi.es/blog/bitcoin-funcionamiento (Consultado: Junio – Julio 2017).

Elperiodicodigital.com (2017): "Banco central advierte que está prohibido el uso de monedas virtuales como el bitcoin", 17 Abril 2017. http://elperiodico-digital.com/2017/04/17/banco-central-advierte-que-esta-prohibido-uso-de-monedas-virtuales-como-el-bitcoin/ (Consultado: 26/06/2017)

Ennis, P. (2016) "The four types of Bitcoin users", 24 Abril 2016. https://www.coindesk.com/four-types-bitcoin-users/ (Consultado: 05/07/2017)

Gomá, I. (2014): "Se puede constituir una sociedad con Bitcoins", 9 Junio 2014. http://hayderecho.com/2014/06/09/se-puede-constituir-una-sociedad-con-bitcoin (Consultado: 29/06/2017).

Gómez, A. (2015): "Bitcoin exento de iva en España", 17 Abril 2015. http://lawandbitcoin.com/bitcoin-exento-de-iva-en-espana/ (Consultado: 30/06/2017).

González Otero, J. M. (2013): "Bitcoin. La moneda del futuro. Qué es, cómo funciona y por qué cambiará el mundo". Unión Editorial, Madrid.

Gorjón, S. (2014): "Divisas o Monedas Virtual: El caso de Bitcoin", Enero 2014. https://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_Bitcoin_enero2014.pdf (Consultado: 26/06/2017).

Guiabitcoin.com (2017): "¿Cómo funciona la seguridad de bitcoin?", http://guiabitcoin.com/funciona-la-seguridad-bitcoin (Consultado: 01/07/2017).

Hall, J. V., & Krueger, A. B. (2016). An analysis of the labor market for Uber's driver-partners in the United States (No. w22843). *National Bureau of Economic Research.*

Hernández, A. (2015): "Las 16 empresas más grande en la minería bitcoin", 17 Agosto 2015. https://criptonoticias.com/mineria/las-16-empresas-mas-grandes-en-la-mineria-bitcoin/#axzz4lQm4TK53 (Consultado: 02/07/2017).

Instituto Nacional de Tecnologías de la Comunicación, https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf (Consultado: Junio - Julio 2017).

Lemos, G. (2017): "Bitcoin, ¿refugio o burbuja?", 23 Enero 2017. http://www.lavozdegalicia.es/noticia/mercados/2017/01/22/bitcoin-refugio-burbuja/0003_201701SM22P3992.htm (Consultado: 26/06/2017).

Metzdowd.com, http://www.metzdowd.com/mailman/listinfo/cryptography (Consultado: 19/06/2017)

Molina, X. (2017): "Las criptomonedas más prometedoras de 2017", 3 Junio 2017. https://es.cointelegraph.com/news/las-criptomonedas-m%C3%A1s-prometedoras-del-2017/es (Consultado: 07/07/2017).

Muñoz, I. (2014): "¿Qué es Bitcoin?, ¿Cómo funciona? Y ¿Dónde se compran?", 13 Febrero 2014. http://computerhoy.com/noticias/internet/que-es-bitcoin-como-funciona-donde-compran-5389 (Consultado: Junio – Julio 2017).

Pérez, I. (2017): "Firma de inversión estadounidense planea introducir Ethereum Classic en el mercado de valores", 9 Marzo 2017. https://criptonoticias.com/mercados/firma-inversion-estadounidense-introducir-ethereum-classic-mercado-valores/#axzz4lrHaBR1J (Consultado: 07/07/2017).

Preukschat, A. (2014): "¿Qué es y de qué sirve el algoritmo SHA-256 en el protocolo bitcoin?", 16 Enero 2014. https://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm (Consultado: 26/06/2017).

Price, R. (2016): "The 18 companies that control bitcoin in 2016", 30 Junio 2016. http://uk.businessinsider.com/bitcoin-pools-miners-ranked-2016-6/#18-p2poolorg-01-1 (Consultado: Junio – Julio 2017).

Queesbitcoin, https://www.queesbitcoin.info/como-utilizar-bitcoin/seguridad (Consultado: 01/07/2017).

Rodriguez, D. (2017): "¿Qué es Bitcoin?" http://www.clublibertaddigital.com/ilustracion-liberal/59/que-es-bitcoin-daniel-rodriguez-herrera.html (Consultado: Junio – Julio 2017).

Rosales, M.S., Maledo, V.R. Y Gallego, G. (2017): "Bitcoin: una visión general", 1 Enero 2017. http://www.revista.unam.mx/vol.18/num1/art11/art11.pdf (Consultado: 26/06/2017).

Rosembuj, T. (2015): "Bitcoin". Barcelona, España. El Fisco.

Sánchez, A.P. (2015): "¿Qué es el clearing bancario?", 2 Febrero 2015. http://www.finanzzas.com/%C2%BFque-es-el-clearing-bancario (Consultado: Junio – Julio 2017).

Sandoval, J. (2015): "Top 10 de países que declaran a Bitcoin prohibido", 28 Mayo 2015. https://criptonoticias.com/colecciones/top-10-paises-bitcoin-prohibido/#axzz4kudY2GdW (Consultado: 04/07/2017).

Sandoval, J. (2017): "Las predicciones para Bitcoin en el 2017", 13 Junio 2017. https://cointelegraph.es/news/predicciones-bitcoin-2017/es (Consultado: 04/07/2017).

semana.com (2016): "¿El bitcoin es legal en Colombia?", 29 Mayo 2016. http://www.semana.com/economia/articulo/bitcoin-legalidad-de-la-divisa-en-colombia/475730 (Consultado: 04/07/2017).

Solís, S. M. (2016): "Bitcoin: guía completa de la moneda del futuro". RA-MA Editorial.

Shadowargel (2017): "HaoBTC anuncia suspensión de su servicio tras medidas del banco popular de china", 14 Febrero 2017. http://www.diariobitcoin.com/index.php/2017/02/14/haobtc-anuncia-suspension-de-su-servicio-tras-medidas-del-banco-popular-de-china (Consultado: 03/07/2017).

Territoriobitcoin.com (2017): "Pool de minería Bitcoin BTC.com anuncia nuevo modo para incrementar ingresos de los mineros", 24 Febrero 2017. https://www.territoriobitcoin.com/pool-de-mineria-bitcoin-btc-com-anuncia-nuevo-modo-para-incrementar-ingresos-de-los-mineros/ (Consultado: Junio – Julio 2017).

The Foundation for Peer to Peer Alternatives, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (Consultado: 25/06/2017)

Tudineroasegurado.com (2016): "¿cuál es el mejor monedero de bitcoin?", 11 Febrero 2016 https://www.tudineroasegurado.com/cual-es-el-mejor-monedero-de-bitcoin/ (consultado: 28/06/2017).

Tuwiner, J. (2017): "Bitcoin: Mining pools", 13 Julio 2017. https://bitcoinworldwide.com/mining/pools (Consultado: 15/07/2017).

Valkenburgh, P.V. (2014): "What is Bitcoin Mining, and Why is it Necessary?", 15 Diciembre 2014. https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary (Consultado: 26/06/2017).

Vera, D. Y Palacios, R. (2006): "Aplicaciones prácticas de la criptografía", Marzo – Abril 2006. https://www.icai.es/contenidos/publicaciones/anales/10_16_AplCriptog_(II-2006)-1235.pdf (Consultado: Junio – Julio 2017).

Vera, D. Y Palacios, R. (2006): "Introducción a la criptografía: tipos de algoritmos", Enero – Febrero 2006. https://www.icai.es/contenidos/publicaciones/anales_get.php?id=1210 (Consultado: Junio – Julio 2017).

Wikipedia (2017): "Satoshi Nakamoto", "Criptografía" "Bitcoin". https://es.wikipedia.org/wiki/Wikipedia:Portada (Consultado: 26/06/2017).

Yelowitz, A., & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, 22(13), 1030-1036.

Zúñiga, A. (2015): "Bitcoin: mucho más que una moneda", Marzo - Abril 2015. http://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-136724.pdf (Consultado: 26/06/2017).