UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

ICADE, Facultad de Derecho y Empresariales

Bitcoins. ¿Revolución o Historia?

Autor: Jaime Sánchez de Diego Martínez-Cabrera
Directora: María Jesús Giménez Abad

Madrid, Junio 2014

Índice

1. Introducción

El **objetivo** del presente trabajo es **estudiar la sostenibilidad en el tiempo de la criptodivisa Bitcoin.** Bitcoin es un fenómeno relativamente nuevo, 2009, que se postula como un start-up tecnológico y ha captado gran atención mediática desde finales de 2013.

Para analizar la supervivencia de la divisa se seguirán una serie de pasos previos a las conclusiones finales. De este modo y en términos generales, el trabajo está **dividido en dos partes fundamentales**.

En primer lugar, una **parte** de carácter puramente **informativo**, esto es, mediante una investigación exhaustiva del sistema se pretende explicar las bases que sustentan la red Bitcoin. Específicamente, la tecnología y algoritmos matemáticos que respaldan el concepto, y la evolución desde sus orígenes en 2009.

De este análisis técnico deriva la segunda y última parte del trabajo. Una vez analizados los pormenores informáticos y principales características del protocolo, se considera que se obtendrá el conocimiento necesario para acometer el resto de la exposición.

La segunda **parte** se correspondería con la agrupación de las **conclusiones** del trabajo. En este contexto, con el entendimiento previo se observará vía gráficas: las cotizaciones, evolución de la red, distribución de la misma y la legalidad. Llegando así al final, dónde se estudiará el valor de Bitcoin como moneda y se realizará un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades). A partir de los dos últimos estudios se elaborará la conclusión final, en la cual se razonará los posibles futuros del protocolo Bitcoin.

Finalmente, quisiera invitar al lector a prestar atención a la primera parte del trabajo que, a pesar de ser compleja debido a las tecnicidades, resulta extremadamente interesante por la innovación y las características del sistema. Se podría decir que el protocolo recoge grandes genialidades.

Concluyendo, la innovación tecnológica es el principal valor que ofrece Bitcoin, siendo la primera divisa digital que soluciona el problema del doble gasto para las transacciones a través de internet, sin recurrir a un tercer agente confiable.

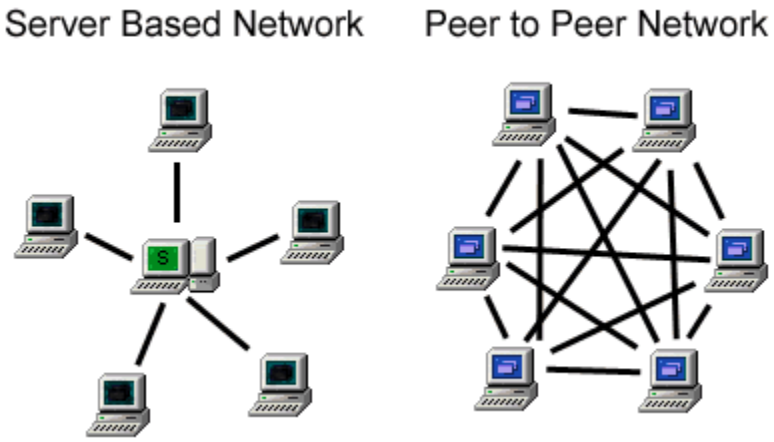
2. Concepto Bitcoin

A. Definición

Bitcoin es una moneda digital criptográfica que usa tecnología P2P para operar sin necesidad de una autoridad central o bancos, creada por Satoshi Nakamoto en 2009. Bitcoin es de código abierto lo que significa que su diseño es público y todo el mundo puede ver el código fuente que sustenta la red.

Para proceder con la explicación del concepto Bitcoin, cabe esclarecer en un primer momento el significado de tecnología P2P (peer-to-peer). Una **red peer-to-peer** permite el intercambio directo de archivos entre diversos ordenadores conectados entre sí. Técnicamente consiste en una red de ordenadores que funcionan como nodos (punto de intersección o de unión) con un mismo comportamiento. Esto es, se actúa simultáneamente como cliente y servidor respecto al resto de nodos que conforman la red y, de esta forma, se produce el intercambio directo de información sin necesidad de un intermediario.

Resumiendo, a diferencia de una red tradicional basada en servidores donde existe un punto central que se encarga del control de la red, P2P conecta directamente dos ordenadores permitiendo que interactúen sin necesidad de intermediación. Esta diferencia se puede observar en las siguientes imágenes:



El peer-to-peer tiene una gran ventaja, la creación de grandes bases de datos de manera gratuita ya que todos los ordenadores conectados pueden descargarse información de los diferentes integrantes de la red. Esta ventaja es la utilizada por el sistema Bitcoin.

La mayoría de las monedas dependen de la confianza de un emisor central que se encarga de avalar la moneda como unidad de valor y preservar el mismo (función de los Bancos Centrales). En cambio, Bitcoin recurre a la base de datos recogida en varios nodos de una red P2P para registrar las transacciones configurando la llamada **cadena**

de bloques o **“block chain”** que se detallará más adelante en el apartado de -funcionamiento.

Por tanto, la diferencia fundamental con las monedas tradicionales es que Bitcoin mediante el uso del P2P se convierte en una moneda descentralizada cuyas transacciones no son rastreadas por ninguna autoridad, sino que esta tarea se realiza a través del colectivo de la red.

B. Funcionamiento

Para comprender el sistema Bitcoin conviene distinguir 3 conceptos diferentes: la **cadena de bloques**, las **transacciones** y el proceso de **minería**.

En primer lugar se hablará de la **cadena de bloques** o **“block chain”** y, para ello, se expondrá el significado de un bloque para posteriormente entender la cadena de bloques.

Un **bloque** es un registro en la cadena de bloques que recoge las confirmaciones de transacciones pendientes. Los bloques son las unidades que forman la cadena de bloques. Los bloques se adhieren a la cadena a través del proceso de minería en un ratio aproximado de: bloque cada 10 minutos, que determina el ratio de crecimiento de la oferta monetaria debido a los incentivos asociados a cada bloque.

La **cadena de bloques** es una contabilidad pública compartida, esto es, todas las transacciones confirmadas se incluyen en la cadena y cada uno de los nodos (ordenadores) de la red Bitcoin contiene una copia de la cadena de bloques. Funciona como un balance de cuentas debido a que el registro de las transacciones permite calcular el saldo gastable y asegurar la correspondencia de pagos y cobros. Para asegurar la integridad y el orden cronológico de la cadena de bloques se utiliza la criptografía.

Antes de continuar con la explicación de las transacciones cabe destacar la importancia de la criptografía en el sistema Bitcoin, haciendo que sea conocida como criptodivisa. La **criptografía** se encarga del estudio de algoritmos, protocolos y sistemas para la consecución de seguridad en los mensajes, la información y la comunicación. En el caso Bitcoin, resulta fundamental a la hora de mantener la seguridad y confidencialidad del usuario así como la integridad de la red. A través de la criptografía se consiguen importantes cualidades en la red Bitcoin:

- **Confidencialidad**: mediante códigos y técnicas de cifrado se garantiza que la información esté disponible solo para usuarios autorizados. Como sabemos todas las transacciones son públicas y están recogidas en la cadena de bloques con lo que cualquier persona puede ver las operaciones y el saldo de una dirección Bitcoin. Eso sí, la identidad del usuario que utiliza determinada dirección no es conocida y las direcciones pueden ser

cambiadas con cada transacción. Por último, las direcciones son claves alfanuméricas generadas por un software determinado funcionando como un "seudónimo" a la hora de efectuarse la operación.

- **Integridad**: referida a que la información es correcta y completa. En este punto tiene un papel fundamental el proceso de minería y las funciones hash criptográficas que se detallarán más adelante*****.

- **Vinculación:** que consiste en la relación de un documento o transacción a una persona o a un sistema criptográfico. Este es el caso de la firma digital y las llaves privadas.

- **Autenticidad:** proporciona mecanismos para verificar la identidad del emisor del mensaje. En un contexto digital sin presencia física, esta cualidad es importante a la hora de entablar transacciones, por consiguiente, se utilizan las funciones hash criptográficas y sus resultantes valores hash.

Una vez expuesto el "sistema contable" o forma de registro de las operaciones de Bitcoins, se va a analizar el significado de las transacciones en este sistema.

Una **transacción** con bitcoins consiste en una transferencia de valores entre monederos Bitcoin, que de ser válida, será confirmada e incluida en la cadena de bloques. Es decir, funciona como un intercambio físico normal con las peculiaridades del contexto digital que dan importancia a la criptografía y el sistema de minería. Por cuestiones de seguridad y para evitar fraudes, los monederos disponen de una **clave privada** que consiste en una **firma criptográfica** que acredita al usuario y le da derecho al gasto de BTC (Bitcoins).

Una vez se efectúa la transacción, ésta es distribuida por todos los nodos de la red para su confirmación y colocación en un bloque. La firma permite que la operación no sea alterada durante este proceso y la cadena de bloques y minería previene el doble gasto. Como se comentaba con anterioridad se genera un bloque cada 10 minutos lo que significa que las transacciones empiezan a ser confirmadas en los 10 minutos siguientes. Se considera que con 6 confirmaciones la transacción es irreversible (1 hora) y, por consiguiente, válida y segura.

Finalmente, la **minería** es el proceso que combina las transacciones y cadenas de bloques. Funciona como un sistema que se utiliza para confirmar las transacciones pendientes para que puedan ser incluidas en la cadena de bloques y como una forma de consenso entre los nodos de la red. Para confirmar las operaciones tienen que ser incluidas en bloques de acuerdo a diferentes reglas estipuladas de cifrado y cobra importancia la llamada **prueba de trabajo**.

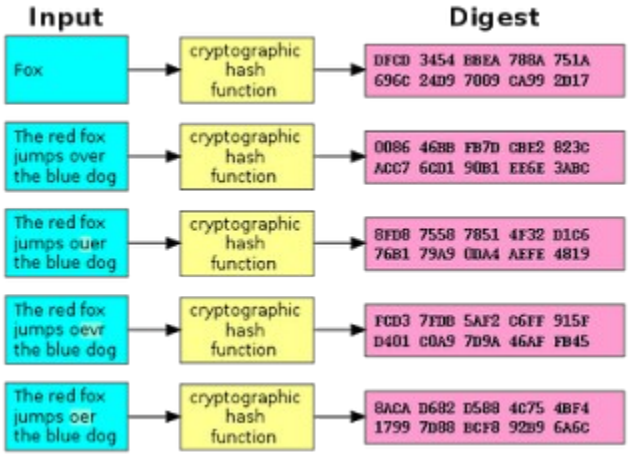
La **prueba de trabajo** o **proof of work** (**PoW**) es un pilar fundamental en la red Bitcoin para el procesamiento de transacciones y la creación de nuevas unidades monetarias. Un sistema PoW se caracteriza por requerir un trabajo del cliente del servicio, que generalmente se traduce en la computación en el ordenador del mismo.

Recapitulando, las transacciones pendientes son lanzadas a la red para ser confirmadas por los nodos, para ser válidas han de constituirse en un bloque. Para ello, Bitcoin produce un desafío o "puzle" que ha de ser resuelto (prueba de trabajo), los mineros tienen que responder a un problema matemático que solo puede ser hallado mediante un sistema de prueba y error, es decir, usando números aleatorios en una ecuación una y otra vez hasta conseguir la respuesta correcta. En conclusión, para conseguir generar un bloque, un minero tiene que registrar prueba de que ha gastado tiempo y energía computacional en la resolución del problema y creación del bloque. La dificultad del problema se calibra de tal forma que un minero pueda resolverlo cada 10 minutos de media. Más adelante se explicarán los incentivos a la minería.

C. Elementos previos al PoW [MINERÍA]

Previo al correcto entendimiento de la prueba de trabajo y la minería, es necesario comprender las funciones hash criptográficas, el nonce criptográfico y el árbol Merkle.

Los **hash** o **funciones hash** son funciones de resumen que utilizan un algoritmo con el que, a partir de una entrada de datos (infinita, cualquier mensaje) producen una salida alfanumérica de longitud fija que resume la entrada, de tal forma que el resultado o **valor hash** solo puede ser obtenido con los mismos valores del input. Cualquier mínimo cambio en la entrada de datos dará lugar a un output diferente. Véase un ejemplo en la siguiente imagen:



Como se puede observar, cualquier cambio en el input nos dará un resumen diferente con la misma longitud pero variables dispares. Las características que una función hash criptográfica ha de cumplir son las siguientes:

- **Determinista:** significa que la función tiene que proveer el mismo resumen dados los mismos datos de entrada, es decir, cada vez que se introduzca “Fox” en la función hash el resultado ha de ser el que aparece en la imagen.

- **Unidireccional:** se refiere a que conocido el valor hash resultante tiene que ser computacionalmente imposible encontrar los valores de entrada. Se puede resumir en funciones fácilmente computables pero imposibles de invertir sin probar todas las posibles variables de entrada. Un ejemplo sencillo podría ser una raíz cuadrada: $\sqrt{18900}$ es fácil de calcular = 137,4772708, una función hash podría darnos los dígitos finales “2708” de los cuales es muy difícil averiguar el numero del que provino, habría que probar muchas combinaciones con los valores iniciales.

- **Eficiente en el cálculo:** la función hash ha de ser fácil de calcular, esto es, dado un determinado input no debe requerir mucha potencia computacional obtener el valor hash final.

- **Compresión:** dado cualquier mensaje inicial y de cualquier amplitud, el resumen tiene que tener una longitud fija. En la imagen se puede observar esta propiedad.

- **Resistencia a la colisión:** una colisión significa que dos valores de entrada diferente resultan en un mismo resumen. En este punto la resistencia se refiere a que la probabilidad de colisión sea baja, lo que implica que el algoritmo sea bueno. Se puede intuir que es matemáticamente imposible la no existencia de colisiones, ya que la función hash trata con un rango infinito de valores como input y un rango finito de salida.

Resumiendo esta información enfocándola en su uso en la red Bitcoin, se podría decir que lo importante de una función hash criptográfica es que sea fácil de producir un valor hash y prácticamente imposible indagar acerca del contenido y los datos de entrada.

En el protocolo Bitcoin los hash se utilizan en dos momentos importantes: en las direcciones y en la minería.

Por un lado, para **generar la dirección pública y las claves privadas.** En Bitcoin se utiliza el algoritmo matemático ECDSA (Elliptic Curve Digital Signature Algorithm) para asegurar que los fondos son gastados por el auténtico dueño de los mismos. También se utilizan los mismos algoritmos que en la minería para maximizar la seguridad de las claves. Se podrían distinguir 3 aspectos: dirección pública, claves privadas y la firma digital.

- **Dirección** o **clave pública:** es aquella con la que un usuario se identifica en la red Bitcoin, el "seudónimo" con el que se opera. Funciona como un email, cualquiera que conozca la dirección puede enviar bitcoins. Es una clave alfanumérica que se genera a partir de la clave privada pero no al revés (unidireccionalidad de las funciones hash). A su vez, la llave pública se utiliza para comprobar si la firma digital es genuina sin necesidad, por tanto, de la divulgación de la clave privada.

- **Clave privada:** es la más importante de todas, es aquella que permite el acceso a los fondos de bitcoins y su gasto en otras direcciones. Se podría equiparar con la clave de cualquier banco, en especial, las requeridas para transacciones por internet.

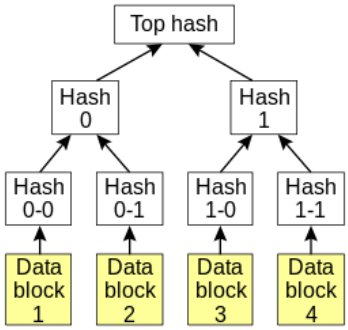
- **Firma digital:** es la forma de demostrar la autenticidad del usuario que realiza una transacción o envía un mensaje. Se obtiene a partir del valor hash del mensaje, encriptado con la clave privada del usuario. El receptor, mediante un algoritmo matemático usará la clave pública para desencriptar el hash y verificar que coincide con el hash del mensaje. De esta forma, se autentifica al usuario sin necesidad de informar sobre la clave privada y, a su vez, si los valores hash no coinciden significa que el mensaje esta alterado o que la clave privada es incorrecta.

Por otro lado, las funciones hash criptográficas se utilizan en la **minería**. El protocolo Bitcoin utiliza el algoritmo SHA-256 y RIPEMD-160 para generar el hash que defina la dificultad del desafío-respuesta en la prueba de trabajo y, por tanto, la necesidad previsible de esfuerzo computacional.

El segundo punto a explicar es el **nonce criptográfico**, un número aleatorio que sirve para asegurar la originalidad de un mensaje, haciendo que el mismo nonce solo se use una sola vez. En Bitcoin los nonces se utilizan para garantizar la seguridad de la cadena de bloques de manera que ésta no sea falsificada. Se podrá observar su uso en la explicación de la prueba de trabajo.

Un ejemplo aclaratorio previo a su explicación en la red Bitcoin podría ser una orden de compra en Internet. Un usuario malicioso obtuviese la información encriptada, sin necesidad de desencriptar, utilizaría el mismo nombre y la misma información de compra para enviar sucesivas ordenes a la empresa. He aquí la utilidad y significado del nonce, la orden de compra tiene un nonce determinado y si la compañía recibiese de la misma persona órdenes con el mismo nonce las descartaría, ya que como se ha dicho el nonce tiene un único uso.

Finalmente, previa a la explicación de la prueba de trabajo se va a tratar el árbol de Merkle. Un **árbol de Merkle** es como un árbol de decisión estadístico compuesto por hashes. Se utiliza por motivos de seguridad, verificación y como forma de comprensión de datos. Véase la siguiente imagen:



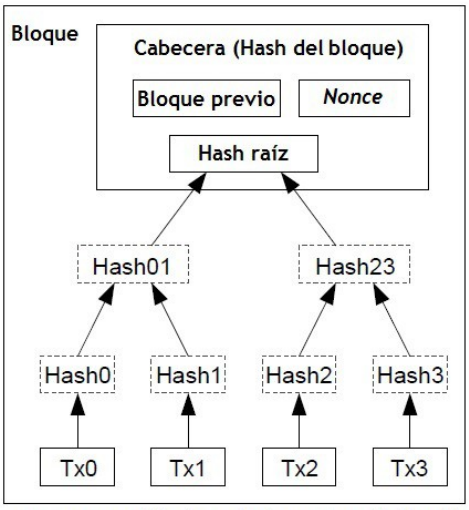
En la parte superior del árbol se encuentra el **"Hash Raíz"** que es el que sirve como forma de verificación de datos. Por ejemplo, un caso con el hash raíz en una operación p2p. A la hora de obtener los diferentes bloques informativos que contiene el mensaje o archivo, se podría obtener el hash raíz de una fuente confiable para poder interactuar con el resto de la red. De esta forma, se recibirá el hash raíz de cualquier usuario con el que se entable relación directa y se comparará con el confiable y, así, las fuentes falsas o con el contenido inadecuado serán rechazadas en post de otras que provean el hash correcto.

Además, sirve como forma de compresión de datos en la medida en que la integridad de cada rama del árbol puede ser comprobada de manera instantánea sin necesidad de la totalidad del árbol, mediante el hash conjunto de datos y la comparación con la raíz. Este hecho se podrá observar en mejor medida con una imagen posterior. Esto es ventajoso debido a que se pueden descargar pequeños bloques de datos de diferentes fuentes asegurando la integridad de los mismos.

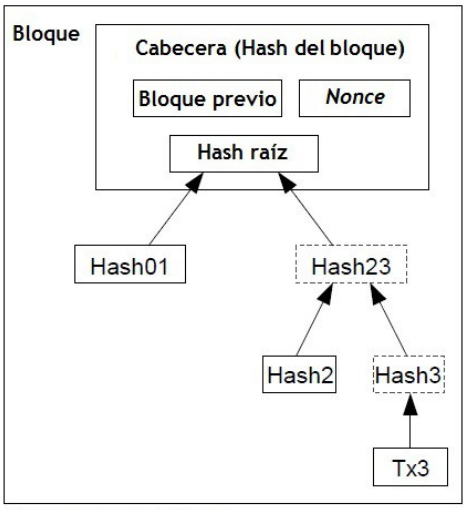
Ahora bien, ¿cómo funciona esto en Bitcoin? Como ya sabemos, las transacciones una vez registradas pasan a la red. Los mineros se encargan de recoger todas estas transacciones y validar la autenticidad de las mismas, es decir, se observan las llaves públicas, privadas y la firma. En ese momento, si las transacciones son válidas el minero las añade a su registro y comienza la creación del bloque.

Para crear un bloque, se hashean las transacciones utilizando el algoritmo SHA-256 y se organizan en el árbol de Merkle. La raíz pasara a formar parte de la cabecera del bloque y, junto al hash del bloque anterior (las razones de esta inclusión serán tratadas posteriormente) y el nonce, se obtendrá el hash del bloque que sirve como identificador. Para la asimilación de esta situación obsérvese la parte izquierda de la imagen siguiente[1]:

1 Nakamoto, S. (Octubre de 2008). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario* .



Transacciones codificadas en *hashes* según un árbol Merkle



Tras cortar Tx0-2 del bloque

La imagen de la derecha nos muestra la función de resumen de la que hablábamos. El árbol de Merkle permite compactar los datos ya que los hashes interiores no necesitan ser guardados.

Por último, una vez obtenido el identificador queda por conseguir una prueba de trabajo válida para añadir el bloque a la “block chain”. Motivo del siguiente apartado.

D. Prueba de trabajo (PoW) [MINERÍA]

En este apartado, debido a su importancia, se explicará el sistema de prueba de trabajo de manera exhaustiva.

La **prueba de trabajo** utilizada en Bitcoin consigue prevenir el doble gasto y se constituye como la esencia de la minería. Comprender este punto conlleva el entendimiento del proceso de **minería**.

Como se expreso anteriormente, un bloque recoge las transacciones confirmadas y posteriormente se adhiere a la cadena de bloques para constituir el “libro mayor contable público”. La prueba de trabajo es el proceso que permite la generación de bloques válidos. Bitcoin utiliza la llamada Hashcash PoW que se basa en un protocolo de desafío-respuesta. Este tipo de protocolo exige un esfuerzo computacional para poder generar un bloque válido.

Al final del anterior apartado vimos como se obtenía la cabecera de un bloque y que el hash de la misma servía como identificador. En este punto del procedimiento entra la prueba de trabajo que consiste en que Bitcoin establece un hash objetivo para la cabecera, de tal forma que empiece con un número determinado de ceros.

La cantidad de ceros requeridos al output de la función hash determina la **dificultad** del problema a resolver. El aumento del número implica la necesidad de una mayor computación de hashes y viceversa. Por ejemplo, el hash del bloque 303.978 fue el siguiente:

000000000000000045146557c537b32f0c36e2ad37814072d82fff5dd49dc443

En este caso se exigían 16 ceros previos al output del hash, siendo el resto de las variables aleatorias. El número de ceros se ajusta cada dos semanas para conseguir la dificultad deseada, este ajuste se entenderá en el apartado de la oferta monetaria.

Por tanto, si ya se había obtenido el identificador de la cabecera mediante el hasheo de la misma, ¿qué pasa si el resultado no tiene los ceros objetivo?

Es ahora donde el nonce criptográfico cobra importancia ya que es la única variable maleable para conseguir el output deseado. Como sabemos la cabecera de un bloque está compuesta por el hash del bloque anterior, el hash raíz y el nonce. Las dos primeras variables son fijas, producto del hasheo previo y el hasheo de las transacciones. El nonce es un número aleatorio que se modifica una y otra vez para conseguir el hash válido.

Por consiguiente, se hashea la cabecera y si el resultado no es el deseado, se modifica el nonce en una unidad (un cambio de tan solo un bit o unidad de texto cambia por completo el resultado de una función hash) tantas veces sea necesario para conseguir el valor objetivo. Por ejemplo, el nonce del bloque 303.978 fue el siguiente: 3705406606.

Finalmente, cuando un minero consigue dar con un hash válido lo confía al resto de la red para su comprobación. Los mineros observan este hash y si es correcto lo incluyen en su copia de la cadena y pasan a buscar el siguiente bloque.

Una vez presentadas las tecnicidades del sistema conviene aclarar el significado del mismo y su utilidad en el protocolo Bitcoin. Para ello, se explicará por qué los mineros intervienen en el proceso (incentivos), qué se consigue (doble gasto y poder computacional), la regla de las seis confirmaciones y la oferta monetaria (funcionamiento en Bitcoin). Por último, se hará un breve resumen de la minería para afianzar la asimilación del concepto.

E. Incentivos

En este punto se van a explicar los incentivos que ofrece la red Bitcoin a las personas para que pongan la capacidad de procesamiento de su ordenador al servicio de la minería y, por consiguiente, asuman el gasto energético que eso supone.

Como se ha podido ver, el proceso de creación de bloques y validación de transacciones es complejo y supone un gasto energético en cuanto a la computación de las operaciones matemáticas que hay que realizar para la incorporación de los bloques a la cadena de bloques.

Para conseguir ordenadores que sustenten la red, Bitcoin recompensa al primer minero (o mineros) que consiga dar con el hash válido de un bloque. Con esta recompensa se consigue que los mineros compitan entre ellos para alcanzar el resultado correcto y obtener el beneficio. Todo ello se traduce en poder computacional para la red.

La recompensa en sus orígenes (2009) constaba de 50 BTC + comisiones por transacción, este premio se va ajustando cada cuatro años a razón de ½, es decir, a la mitad (esto no afecta a las comisiones). Actualmente el premio por dar con un bloque válido supone 25 BTC + comisiones.

Por tanto, una vez se ha creado un bloque y se ha obtenido la prueba correspondiente mediante la computación de hashes, el minero incluye en dicho bloque una transacción con el importe de la recompensa a su dirección Bitcoin.

Dada la computación necesitada y la especialización del sistema un minero individual es poco probable que obtenga el resultado. Esto hace que se unan diferentes individuos en lo que se conoce como piscinas de mineros, donde se ponen varios ordenadores a trabajar conjuntamente y, en caso de obtener la recompensa, ésta es distribuida equitativamente entre los mismos de acuerdo a la capacidad computacional aportada.

La minería crea lo equivalente a una lotería, la prueba de trabajo incluye el factor aleatorio en la obtención del hash válido y el % de cómputo de un ordenador sería igual a los tickets de lotería, esto es, cuando más poder de procesamiento, más posibilidades de dar con la combinación ganadora. Este sistema hace que sea sumamente difícil para una persona incluir varios bloques consecutivos en la cadena (es poco probable ganar la lotería, pero menos probable ganarla sucesivamente). De esta forma, nadie controla lo que está incluido en la cadena, ni puede revertir sus propios gastos mediante el reemplazo de bloques (doble gasto, tratado en el siguiente apartado). La probabilidad de superar este sistema será analizada en la regla de las seis confirmaciones.

Con motivo de ofrecer una visión sobre la dificultad de este proceso, véase la probabilidad de un único hash resolviendo un bloque a los niveles actuales de dificultad: 0.000000000000000000002226791[2], siendo la dificultad de: 10.455.720.138,485 intentos de hash hasta dar con el valor objetivo.

Otro detalle importante en lo referente a las recompensas de la minería, es que los BTC obtenidos no pueden ser gastados hasta que se hayan añadido 100 bloques

2 *Block explorer*. (s.f.). Recuperado el Mayo de 2014, de http://blockexplorer.com

nuevos a la cadena. Esta medida tiene la finalidad de evitar que los BTC generados por un bloque sean gastados, por si se da el caso de que el bloque es descartado por no pertenecer a la cadena más larga. El concepto de cadena más larga será tratado en la siguiente sección en la parte de bifurcaciones.

Para finalizar con el tema de incentivos queda por explicar de dónde derivan las comisiones y la segunda funcionalidad de la recompensa. Las comisiones provienen de la parte que paga en una transacción Bitcoin, son voluntarias y sirven para agilizar el proceso de confirmación mediante la incentivación a los mineros (los mineros no están obligados a incluir una determinada transacción en el bloque que intentan resolver, la existencia de comisiones prioriza, por consiguiente, su inclusión en un bloque).

Concluyendo, la recompensa tiene una segunda funcionalidad que es la de poner en circulación nuevas unidades monetarias. El premio por la creación de bloques es la forma de “acuñar moneda” del sistema ya que no existe una entidad reguladora que decida la cantidad de dinero que producir. Esta parte se verá en profundidad en el apartado de la oferta monetaria.

F. Doble gasto y poder computacional

El objetivo de esta sección es expresar dos cuestiones importantes que consigue el protocolo Bitcoin mediante la utilización de su sistema de minería. Primeramente, tratemos el tema del **poder computacional**.

En un sistema monetario normal cualquier persona puede acudir a un ATM o cajero automático y extraer dinero para realizar una transacción. En este proceso el banco estaría pagando por la energía consumida por mantener el cajero operativo y regular la extracción del dinero.

En Bitcoin también se necesita este poder computacional para mantener la red operativa 24/7, es decir, para que se puedan realizar transacciones en cualquier momento, es necesario que haya mineros validando las mismas e integrándolas en la cadena de bloques mediante la creación de un bloque. Mediante el sistema de prueba de trabajo se consigue esta actividad computacional. Como se veía en el punto anterior, los mineros son recompensados por su actividad, lo que supone un incentivo para que mantengan sus ordenadores operativos.

En segundo lugar, veamos que significa **doble gasto** y que hace Bitcoin para evitarlo.

En un **intercambio físico** entre un cliente y una tienda, el primero provee el dinero y recibe a cambio el producto requerido. Por tanto, el billete o monedas utilizadas solo existen en un solo lugar, esto es, el billete que se ha utilizado para comprar el producto no puede volver a ser utilizado por la misma persona ya que se encuentra en la caja registradora de la tienda.

En una **extracción** monetaria de un **banco** o cajero, lo que ocurre es que antes de la retirada de efectivo el banco se encarga de comprobar el estado de la cuenta para la disposición de fondos. Una vez retirada la cantidad de dinero acorde al saldo de la cuenta, de nuevo el banco se encarga de ajustar el balance para que no ocurra un doble gasto, es decir, que no se utilice el mismo dinero dos veces.

En la **red Bitcoin** no existe una autoridad central, nadie tiene la autoridad para actualizar los estados de las cuentas. Lo que impide a un usuario registrar dos transacciones diferentes con el mismo dinero es el trabajo y el consenso de los mineros.

Observemos que se necesitaría para llevar a cabo una operación fraudulenta de estas características. Para ello, es necesario retomar conceptos previos de la cadena de bloques.

Como analizábamos anteriormente, la cabecera de un bloque está compuesta por una serie de elementos. El elemento que ahora nos ocupa es el **hash del bloque anterior**, al incluirlo en el nuevo bloque se están conectando los mismos, registrando toda la información previa.

Supongamos que un usuario malicioso intentara efectuar el doble gasto, esto es, realizar una transacción que es confirmada por la red y, posteriormente, con el mismo dinero realizar otra transacción. Para conseguirlo, tendría que alterar la transacción que ya está registrada.

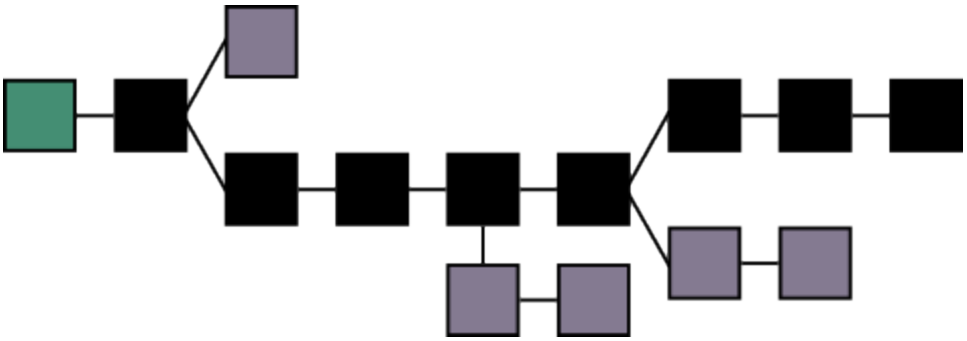
Con lo que, una mínima alteración de una transacción supondría la alteración del hash, con las consecuentes alteraciones de las ramas del Árbol Merkle hasta la Raíz. Una nueva Raíz supondría un nuevo hash del bloque que es muy poco probable que sea válido (por la prueba de trabajo). En este punto, nuestro usuario podría seguir queriendo realizar el fraude del doble gasto. Para ello, tendría que realizar el esfuerzo computacional de la prueba de trabajo, dar con un hash correcto y enviar el nuevo bloque a los nodos. Digamos que este bloque es el número 2.

El objetivo del fraude es que el nuevo bloque sea aceptado y, por tanto, el doble gasto sea efectivo. Pero debido a que cada bloque incluye el hash del anterior, el nuevo bloque 2 modifica el hash del bloque 3, haciendo que sea necesario volver a hashearlo, este proceso continua a lo largo de la cadena.

Se daría entonces una situación en la que a partir de ese bloque 2 existen dos continuaciones de la cadena. La continuación honesta ha seguido avanzando, así que el atacante tendría que hashear y procesar los bloques a mayor velocidad que el resto de la red. Es decir, el doble gasto solo podría ser posible si consigue un poder de computación del 51%. Esta amenaza de una entidad o usuario con el 51% del poder de hasheo o minado se explicara posteriormente.

Aprovechando la explicación de esta situación de doble gasto que produce dos continuaciones de la cadena, analizamos que ocurre con estas bifurcaciones.

Las **bifurcaciones** o **fork** no solo son producidas por problemas de doble gasto, sino que podría darse el caso de que dos mineros obtienen la solución de un bloque relativamente al mismo tiempo. Al enviarse a la red, el resto de mineros tendría que decidir en qué cadena operar ya que los problemas matemáticos van a ser diferentes. El poder de procesamiento equivaldría a votos en este contexto, debido a que la cadena de mayor longitud (referida a esfuerzo computacional requerido) prevalecería. Obsérvese la siguiente imagen:



En la imagen, el bloque verde equivale al bloque génesis (el origen de la cadena por Satoshi) y la cadena principal sería la sombreada en negro. Los bloques morados serían aquellos bloques producidos por cualquier razón que no contaran con el apoyo de la red, se les denomina bloques huérfanos porque no forman parte de la cadena principal.

Desde el punto de vista de un minero se puede comprender mejor esta regla de la cadena de mayor longitud. El coste de oportunidad de operar en una cadena minoritaria (con menor capacidad de procesamiento) es muy grande, ya que se consume energía sin tener posibilidad de acceder a la recompensa, por consiguiente, los mineros eventualmente abandonan la cadena minoritaria para trabajar en los problemas de la cadena principal.

Por último, es de recibo destacar que las transacciones que se encuentran en bloques de la cadena más corta, se transforman en transacciones pendientes para su inclusión en un bloque de la cadena principal.

G. La recomendación de las seis confirmaciones

La recomendación considera que cuando se han recibido seis confirmaciones la transacción es irreversible. Inicialmente hay posibilidades de que la transacción se revierta, lo cual ocurriría en casos de una bifurcación de la cadena de bloques. Cada

confirmación implica que un nuevo bloque ha sido añadido a la cadena y, por cada una de ellas, la probabilidad de reversión de la transacción se reduce exponencialmente.

Esta recomendación se basa en la idea de una posible bifurcación en la cadena, con dos ramas compitiendo por convertirse en la principal. Se considera que tras 6 bloques nuevos la transacción será difícilmente revertida porque se encontrará en la cadena más larga.

En el documento original de Bitcoin, escrito por Satoshi Nakamoto, se pueden encontrar los cálculos de la probabilidad de que un atacante con un 10% del total del poder computacional de la red, pueda conseguir un doble gasto exitoso. Véanse los resultados teniendo en cuenta que: “q” es el porcentaje de la red controlado por el atacante; y “p” es la probabilidad de que el atacante llegue a alcanzar a la cadena honesta desde “z” bloques atrás.

q =0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173

Como se puede observar un usuario malicioso con el 10% de la red e intenciones de doble gasto, tendría una probabilidad de 0.024% de tener suerte y superar a la cadena honesta tras 6 bloques. De aquí surge la recomendación de las seis confirmaciones. También se puede ver que cada bloque reduce la probabilidad exponencialmente.

H. La oferta monetaria

En este apartado se ofrecerá el funcionamiento de la oferta monetaria en Bitcoin, la descentralización de la criptodivisa hace que sea muy importante para estudiar la sostenibilidad de la misma. El objetivo es ofrecer las bases teóricas del mismo para tratar más adelante los problemas y ventajas que supone.

Es importante destacar que los **problemas** más sonados a **largo plazo** que Bitcoin tiene que acometer hacen referencia a la **seguridad** y al **funcionamiento de la oferta monetaria**. Los pilares en los que se sustenta la seguridad de la red han sido tratados a lo largo del texto, si bien queda por aclarar explícitamente las críticas a favor y en contra en lo referente a la seguridad.

Antes de explicar cómo se organiza la oferta monetaria en Bitcoin, conviene analizar en líneas generales el funcionamiento de una economía centralizada respecto al tema. La exposición se dividirá en **creación monetaria** y **oferta monetaria**.

En una **economía centralizada** el dinero es creado directamente por los bancos centrales o a través de préstamos por los bancos comerciales. Tengamos en cuenta la **ecuación fundamental** de la oferta monetaria:

$$M = m*BM$$

M = Oferta monetaria (dinero disponible en la economía)
BM = Base monetaria (dinero a partir del cual se genera la oferta monetaria)
m = Multiplicador monetario (referente a la creación de dinero mediante reserva fraccionaria)

En la ecuación se encuentran recogidas las dos formas de **creación monetaria** en un sistema centralizado. Por un lado, la creación directa de dinero de los **bancos centrales** constituye la **base monetaria** y es la herramienta principal usada para controlar la oferta monetaria, con objetivos de un cierto tipo de interés. Se puede observar fácilmente que un aumento de la base monetaria supone un mayor incremento de la oferta, debido al multiplicador y viceversa.

Por otro lado, los **bancos comerciales** crean dinero a través de los **préstamos**, sistema conocido como banca de **reserva fraccional**, esto es, se mantiene una reserva equivalente a un porcentaje de los depósitos de un cliente y el resto del monto se utiliza en las operaciones del banco como los préstamos.
El **multiplicador monetario** dado un ratio de reservas, calcula la expansión o aumento de la cantidad de dinero que se produce a partir de un depósito inicial, es decir, nos permite calcular la cantidad máxima de dinero creado con la reserva fraccionaria. Por ejemplo: con un multiplicador de 100 (reservas del 1%), un depósito de 10€ (aumento BM) acaba creando 1.000€.

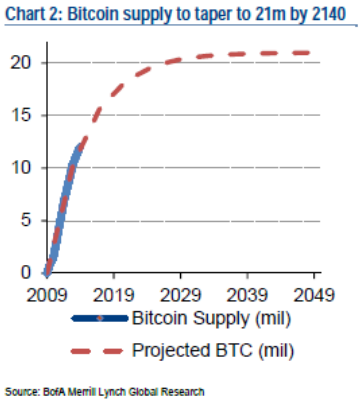
En este contexto, la **oferta monetaria** es impredecible y dependerá de las políticas monetarias implementadas por bancos y gobiernos. Asimismo, la base monetaria es infinita en el sentido que puede seguir creciendo ilimitadamente, los límites a su crecimiento están basados en la autoridad gubernamental y bancaria, pero no son cuantificables a largo plazo y el ratio de crecimiento de la misma es impredecible.

En el **protocolo Bitcoin** la creación de dinero se hace a través de la minería y los préstamos peer-to-peer.

En el punto de incentivos ya veíamos como la **minería** era la forma de creación de unidades monetarias mediante la recompensa a los mineros. Por tanto, nadie puede crear dinero y aumentar la base monetaria más allá de las monedas creadas en la minería. Esto hace que el ratio de crecimiento y la base monetaria sean previsibles.

Además, la otra forma de creación de dinero es igual a la de una economía centralizada, es decir, mediante **préstamos**, con la peculiaridad de ser a través de un sistema P2P y no un intermediario financiero. El funcionamiento de este sistema excede el motivo del trabajo, basta decir que estas prácticas, aun existiendo en la actualidad en Bitcoin, no están muy desarrolladas y cuentan con pocas plataformas hábiles. Por consiguiente, se podría asumir que la creación de dinero por esta vía es baja en estos momentos. Si bien podrían ser más relevantes en el largo plazo.

Resumiendo, la **oferta monetaria** en Bitcoin es finita y el número de bitcoins que existirán nunca sobrepasará los 21 millones, cantidad a la que se llegará en 2140. Esta cantidad de oferta podrá ser superada debida al sistema de reserva fraccionaria. Obsérvese la siguiente imagen[3]:



Tres apuntes respecto a esta realidad:

El límite de 21 millones se obtiene a partir del ratio de creación de bloques, 6 a la hora en promedio, ajustándose la dificultad cada dos semanas (aumento/disminución de ceros objetivos en la prueba de trabajo) para asegurar este ratio. Y a partir del descenso geométrico de ½ cada 4 años en la generación de bitcoins.

Aunque la oferta sea limitada, el BTC es ampliamente divisible al ser una moneda digital. Actualmente, la menor fracción de bitcoins que se puede enviar en una transacción constituye un *Satoshi* y equivale a 0.00000001 BTC. En el futuro el protocolo podría ser actualizado respecto a esta cuestión permitiendo mayores subdivisiones en caso de ser necesario.

Por último, la parte más importante y objeto de gran discusión sobre Bitcoin, es la **tendencia deflacionaria** de la moneda, esto es, el límite a la oferta monetaria hace que sea una moneda a prueba de inflación (a diferencia de las monedas centralizadas) pero, a su vez, el hecho de que la oferta monetaria no se pueda expandir hace que la

3 Woo, D., Gordon, I., & Iaralov, V. (2013). *Bitcoin: a first assesstment.*

moneda esté sujeta a deflación en caso de un aumento considerable del negocio. Los inconvenientes de la deflación se estudiarán en el análisis DAFO.

Para aclarar porque es una moneda con tendencia deflacionaria hay que comprender el siguiente esquema. Una deflación es una disminución en los precios de los bienes y los servicios. La oferta monetaria fija de Bitcoin hace que llegado al límite, si aumenta la demanda de la moneda, su valor se verá incrementado. Si el precio de BTC sube en lo relativo a una divisa como puede ser el €, significa que mas € serán intercambiados por cada BTC. Si expresamos esta situación en un ambiente de bienes y servicios el resultado es el siguiente:

Ejemplo deflación: un producto x cuesta 300€, la cotización de BTC está a 1 BTC = 150€, con lo que, por 2 BTC se adquiere el producto. Si la demanda aumenta y no se crea más dinero, el valor de BTC aumenta, pongamos una cotización de 1 BTC = 300€. Por tanto, el precio de comprar nuestro producto x baja a 1 BTC.

Esta regla se mantendría en el tiempo, cuanta más demanda, mayor valor de los BTC y menor es el precio de los artículos a comprar, ya que el valor del producto en la moneda fiat (€, $...) seguiría siendo el mismo.

I. Resumen

Las transacciones se encuentran organizadas en un Libro Mayor que sirve de contabilidad pública llamado la cadena de bloques. Una copia de la cadena se encuentra en cada nodo de la red Bitcoin y la seguridad de la misma se basa en técnicas criptográficas.

Cuando se realiza una transacción, ésta es confiada a la red para su validación y confirmación. Los mineros se encargan de comprobar estas transacciones y generan bloques agrupándolas. Para generar un bloque es necesario realizar una prueba de trabajo que se traduce en un esfuerzo computacional para resolver un problema matemático, este esfuerzo consiste en un sucesivo procedimiento de prueba y error.

Se genera un bloque cada 10 minutos aproximadamente, la dificultad de creación de un bloque se ajusta cada dos semanas para asegurar este ratio. El minero o mineros (piscinas de mineros) que consigan generar un bloque reciben una recompensa compuesta por una cantidad de BTC mas las comisiones pagadas por el emisor de una transacción, la recompensa en bitcoins se modifica cada cuatro años a razón de 1/2. Estas unidades monetarias constituyen el ratio de crecimiento de la oferta monetaria, que es finita y tiene un límite de 21 millones de monedas.

3. Evolución del Bitcoin

En esta sección se va a hacer un recorrido cronológico de los hechos más relevantes que han afectado a Bitcoin. Además de la información intrínseca que se encuentra recogida en la cronología, este análisis nos permitirá comprender posteriormente cambios en la cotización de Bitcoin.

A lo largo del recorrido se explicarán ciertos conceptos financieros que irán apareciendo y se hará especial hincapié en las brechas de seguridad soportadas. La aceptación de BTC por nuevos negocios no será tratada, siendo solo mencionables los más conocidos.

- **Agosto, 2008:** La página principal del protocolo, **Bitcoin.org**, es registrada. Se obtiene un dominio web para la misma.

- **Octubre, 2008:** Satoshi Nakamoto publica el documento original de Bitcoin, titulado: **"Bitcoin: A Peer-to-Peer Electronic Cash System"**. La gran innovación es la solución del problema del doble gasto sin la necesidad de un tercer agente en una transacción, esto es, existían monedas digitales previas al Bitcoin (Facebook credits, Microsoft points, e-gold…) pero solucionaban el problema del doble gasto mediante la intermediación.

- **Noviembre, 2008:** El proyecto Bitcoin es registrado en **Sourceforge.net** que es una página web cuyo objetivo es desarrollar y distribuir software de código abierto. Sirve como una base de datos para este tipo de software.

- **Enero, 2009:** Se mina el **bloque génesis**. El primer bloque de la red es obtenido lo que marca el comienzo real de la criptodivisa. También se lanza la **primera versión** del software Bitcoin V 0.1 y se realiza la **primera transacción**.

- **Octubre, 2009:** New Liberty Standard publica un **tipo de cambio** para Bitcoin, siendo su valor de US$ 1 = 1.309,03 BTC. La ecuación utilizada para obtener esta tasa se basa en el coste de electricidad requerido para operar con un ordenador durante un año. Consistiendo en dividir $1 por la cantidad media de electricidad utilizada para ejecutar un ordenador durante un año (Q), multiplicado por el coste medio residencial de la electricidad en USA del año anterior (CMe), dividido por 12 meses y dividido por el número de BTC generado por mi ordenador en los últimos 30 días (nB). $1/Q·CMe/12/nB

- **Diciembre, 2009:** primera vez que se produce un **incremento de la dificultad** de minado. Esto implica que más usuarios acceden a la red y, por tanto, mayor poder de computación al servicio de la minería. El aumento de dificultad permite que el ratio 6 bloques a la hora se cumpla.

- **Febrero, 2010:** nace el primer organismo de **cambio de divisas** de Bitcoin, llamado The Bitcoin Market. Actualmente existen varias organizaciones que permiten el cambio de divisa, es decir, que permiten intercambiar BTC por otras monedas de curso legal. Cabe destacar que la existencia de estas instituciones implica una tercera parte en la red Bitcoin que opera con funciones similares a un banco. Por consiguiente, Bitcoin aconseja a sus usuarios que investiguen estas organizaciones para comprobar si son confiables, ya que la red y sistema son seguros, pero los usuarios y organizaciones están sujetos a fraude informático si no se toman precauciones.

- **Mayo, 2010:** se produce la **primera transacción en el mundo real**. Un programador intercambia 10.000 BTC por pizza. Hay que tener en cuenta que cada pizza costaba $25 USD y que esos bitcoins podrían haberse intercambiado en The Bitcoin Market por $41. Lo relevante de la situación es que se produce el primer pago en BTC.

- **July, 2010:** se establece en Tokyo (Japón) el broker de bitcoins **Mt. Gox**, uno de los más importantes en el universo Bitcoin como se irá viendo a través de la historia. Además, Bitcoin es mencionado en **Slashdot** un sitio de noticias principalmente orientado a la tecnología. El conocimiento por parte de los usuarios empieza a aumentar.

- **Agosto, 2010:** una **vulnerabilidad** afecta al sistema Bitcoin. Las transacciones no se verificaban en ese momento previa inclusión a la cadena de bloques. Esta vulnerabilidad se explota con la creación de 184 billones de BTC en una transacción. Finalmente, se detecta el fallo del sistema el cual es arreglado y, a su vez, la transacción es detectada y borrada.

- **Septiembre, 2010:** el incremento constante de la dificultad en la minería y el constante aumento de la competitividad generan la **primera piscina de mineros**, Slush's pool. De esta forma, la colaboración entre mineros permite una mayor posibilidad de generar un bloque y recibir la recompensa, que será dividida entre los miembros de la piscina.

  En estas fechas también se encuentra otro **fallo** en la red, relacionado con las **microtransacciones**. Mediante el envío continuado de pocos BTC entre direcciones diferentes se podría ralentizar la generación de bloques y saturar el sistema. Este fallo deriva en el lanzamiento de la Versión 0.3.13 de Bitcoin.

- **Octubre, 2010:** tiene lugar la **primera transacción garantizada** entre usuarios del foro Bitcoin. Esto es, una transacción entre dos usuarios garantizada por un tercero. Actualmente existen organizaciones que garantizan las transacciones a cambio de una comisión como: btcrow.com.

Además, se registra **#bitcoin-otc** en canales gratuitos IRC como mercado over-the-counter para el trading de Bitcoin. Hay que distinguir dos puntos en este hecho: un **mercado over-the-counter (OTC)** consiste en la negociación de instrumentos financieros directamente entre dos partes, sin la intermediación de ninguna bolsa de valores; I**RC (Internet Relay Chat)** es un sistema de comunicación en tiempo real por medio de la escritura, permite el debate entre dos o más personas. Todas las personas conectadas a un canal determinado pueden interactuar entre sí.

Con la creación de este mercado se produce la **primera venta en corto** con BTC, mediante el préstamo de 100 BTC entre dos usuarios. La venta en corto consiste en vender un instrumento financiero que no se posee, para recomprarlo y devolverlo posteriormente, con la expectativa de una bajada del valor de cotización. **Ejemplo:** La cotización esta a 1 BTC = $10, Alice presta a Bob 100 BTC, Bob vende los BTC obteniendo $1.000 con la esperanza de una devaluación del BTC. Posteriormente, la cotización baja a $7, Bob recompra los 100 BTC a un precio de $700 y se los devuelve a Alice, obteniendo un beneficio de $300 por su venta en corto. En el caso de una subida en la cotización sería Alice la que recibiría la plusvalía de la operación.

- **Diciembre, 2010:** se realiza la **primera transacción entre dos móviles**. El monedero Bitcoin aparece como aplicación móvil. A su vez, la dificultad aumenta excediendo los 10.000 hasheos para alcanzar el valor objetivo. Con este dato se puede observar la evolución de la red que pasa, en dos años, de una dificultad de 1 en el bloque génesis a 10.000. El progreso de la dificultad podrá ser observada en una gráfica posterior.

Durante estas fechas también se realiza el primer contrato de una opción call en el mercado OTC. Una **opción call** da derecho a un comprador a obtener un activo a un precio determinado en una fecha previamente establecida, a cambio del pago de una prima. Por tanto, si el mercado tiene tendencia alcista y se supera el precio de ejercicio (precio establecido en el contrato) el comprador ejercerá su derecho comprando los BTC a menor precio y vendiéndolos a precio de mercado. En el caso contrario (precio de mercado menor al precio de ejercicio), no se ejercerá la opción y el vendedor obtendrá un beneficio equivalente al importe de la prima.

- **Febrero, 2011:** se funda **Silk Road** un mercado negro para el comercio de drogas en línea, las transacciones se hacen en BTC debido a su anonimato. La web funciona como eBay o Amazon en concepto de drogas, aprovechándose de los beneficios del BTC y de otro proyecto tecnológico conocido como Tor (cuyo objetivo es conseguir la imposibilidad de rastreo de los usuarios en internet, anonimato). Este hecho pone de manifiesto uno de los problemas de Bitcoin referente al comercio ilegal y al blanqueo de dinero.

Otra cuestión relevante es que se alcanza en este mes la paridad con el dólar, es decir, 1 BTC = $1 USD en MtGox. Esta paridad conlleva un mayor tráfico en la web de Bitcoin, así como el aumento de los artículos periodísticos explicando el concepto. Todo esto se resume en un mayor conocimiento de Bitcoin.

- **Marzo, 2011:** el fundador de MtGox, Jed McCaleb, vende la empresa a la compañía japonesa Tibanne Co., Ltd.

  En este mes se abren dos nuevos mercados al intercambio de BTC. En primer lugar, **Britcoin** que permite intercambiar BTC por libras esterlinas británicas. En segundo lugar, **Bitcoin Brasil** que se convierte en el primer mercado de intercambio de BTC por reales brasileños.

- **Abril, 2011:** abre **Bitmarket.eu** convirtiéndose en un organismo de cambio de divisas entre BTC y otras monedas como el euro, el zloty polaco, el franco suizo, el rublo ruso… Como se puede observar en las aperturas de estas casas de cambio, el Bitcoin empieza a ganar popularidad.

  Durante este periodo también se vende el primer contrato de una opción put en el mercado OTC. Una **opción put** es el instrumento financiero contrario a una call, es decir, el comprador tiene el derecho a vender un activo a un precio específico en una fecha predeterminada, a cambio del pago de una prima. Se utiliza para protegerse frente a bajadas del mercado, ya que si el precio de cotización es menor que el precio de ejercicio, el comprador ejercerá su derecho y venderá los activos a un precio superior al del mercado.

  Por último, el negocio VirWox abre sus puertas al Bitcoin. **VirWox** es el intercambiador líder de monedas virtuales, es decir, del dinero utilizado en plataformas o mundos virtuales.

- **Junio, 2011:** hay una serie de acontecimientos importantes que suceden en este mes. Por un lado, **WikiLeaks**, la conocida página web que muestra documentos filtrados de interés público, comienza a aceptar donaciones en forma de Bitcoin.

  Por otro lado, se producen una serie de **robos** que empiezan con un usuario del foro Bitcoin reclamando que 25.000 BTC han sido extraídos de su cartera (US $375.000). Días después de la noticia se informa de la violación del sistema de seguridad de MtGox, que resulta en la fuga de información de 60.000 cuentas (nombres de usuario, direcciones de email y hashes contraseña). La base de datos es accedida a través de una cuenta de administración hackeada que realizaba numerosas transacciones y finaliza con el parón del servicio de la empresa durante siete días. Otras organizaciones como TradeHill y Britcoin dejaron de prestar servicio de trading mientras las medidas de seguridad eran revisadas. Estos hechos se reflejarán en la cotización (analizada más adelante) y ponen de manifiesto los fallos de seguridad a los que se enfrentan los usuarios de las monedas digitales.

  Finalmente, The Electronic Frontier Foundation **(EFF)**, definida a sí misma como una organización sin ánimo de lucro que defiende los derechos de los usuarios en el mundo digital, deja de aceptar donaciones en BTC alegando incertidumbre legal. Estos aspectos de legislación serán tratados en el apartado del análisis DAFO.

- **Julio, 2011:** el tercer broker más grande de Bitcoin, **Bitomat**, pierde acceso a un monedero de fondos de 17.000 BTC. La información de la cuenta estaba guardada online en un sistema de datos que al desconectarse de la red provocó la pérdida de los datos que permitían el gasto de BTC.

- **Agosto, 2011:** el procesador de transacciones de **MyBitcoin** es **hackeado** perdiéndose 150.000 BTC por valor de US $2 millones. MyBitcoin es el primer servicio de monedero online de la red Bitcoin en el momento. Se puede observar el problema de seguridad de los agentes que operan en el protocolo Bitcoin con todos los hechos que se están presentando.

- **Febrero, 2012: TradeHill** el segundo organismo de intercambio de divisas (tras MtGox) por BTC anuncia el **cese de su actividad**. El CEO Jered Kenna alega dos razones para este cierre: por un lado, el incremento de la regulación y, por otro lado, la pérdida de $100.000 de una de las cuentas por el conflicto con un procesador de pago.

- **Marzo, 2012: Linode** un servicio web de alojamiento de datos es **hackeado**, la brecha de seguridad permite el robo de información sobre ciertas cuentas de Bitcoin, siendo robados 46.000 BTC por valor de $228.000.

- **Mayo, 2012:** el **FBI** realiza un documento expresando su preocupación acerca del uso de los Bitcoins en actividades ilícitas, como la compra de productos ilegales o el blanqueo de dinero. El lector recordará la mención a Silk Road y el aprovechamiento de las peculiaridades del sistema para realizar una actividad ilegal.

  Los **robos** continúan este mes con **Bitcoinica** siendo hackeada y perdiendo 18.000 BTC valorados aproximadamente en $90.000. Bitcoinica fue objeto de robo en el mes de marzo en el incidente de Linode (43.000 BTC de los 46.000 BTC), con este segundo robo la compañía es demandada por sus usuarios y cierra sus puertas online.

- **Septiembre, 2012:** una de las entidades estadounidenses más representativas de intercambio, **Bitfloor**, pierde una cantidad considerable de BTC debido a un **hack** del sistema. 24.000 BTC por valor de $250.000 son robados y las operaciones de intercambio quedan paralizadas.

  Durante este periodo la Securities and Exchange Comission **(SEC)** de Estados Unidos anuncia la investigación de una organización que opera con Bitcoins por la posibilidad de que se esté usando un esquema Ponzi o estafa piramidal. Finalmente, se descubre que ese es el caso, Bitcoin Saving and Trust ofrecía un 7% de interés semanal. Un **esquema Ponzi** es una operación fraudulenta en la que se paga a los inversores los intereses con el mismo dinero invertido por ellos, así como el de nuevos inversores, siendo el caso más sonado y reciente la estafa de Madoff.

Por último, otro hecho importante es la creación de **The Bitcoin Foundation**, organización cuyo objetivo es estandarizar, proteger y promover Bitcoin. De esta forma, se ponen al servicio del protocolo equipos de desarrollo y supervisión.

- **Noviembre, 2012:** se produce el primer reajuste de las recompensas por bloque, es decir, a partir de este mes la recompensa por la creación de cada bloque se reduce a la mitad siendo 25 BTC.

- **Diciembre, 2012:** aparece la primera institución de cambio de divisas (BTC - €) con **licencia de banco** y bajo la regulación del marco europeo, **Bitcoin Central**. La organización garantiza los depósitos de sus clientes hasta cierto punto y, además, ofrece la seguridad de ser un organismo amparado bajo la legalidad del marco europeo. Por tanto, no soporta la incertidumbre y el riesgo de la regulación como gran parte de la red Bitcoin.

- **Marzo, 2013:** se produce otra intrusión informática, esta vez en el intercambiador BitInstant que resulta en la pérdida de BTC por valor de $12.000.

Además, The Financial Crimes Enfocement Network **(FinCEN)** de los Estados Unidos publica un documento en el que ofrece una definición y mínima **regulación** de las **monedas virtuales**. Se considera que este tipo de moneda tiene un valor equivalente en dinero real o actúa en sustitución del mismo. Se requiere registro de ciertas actividades como negocios de transmisión de dinero y éstos están sujetos a ciertas responsabilidades.

A su vez, se produce una situación muy relevante, una **bifurcación en la cadena de bloques** que provoca una parada en las transacciones hasta que se solvente el conflicto. La bifurcación se origina por la actualización del software de Bitcoin. De tal forma que el software antiguo (versión 0.7) no podía leer un bloque al igual que la nueva versión 0.8. A partir de esta situación, se divide la cadena de bloques entre los usuarios de la versión 0.7 y 0.8, que trabajan en bloques diferentes como explicábamos anteriormente.

La 0.8 tenía mayor poder computacional y llevaba ventaja a la otra versión, pero si esta cadena salía victoriosa todos los usuarios de la red tendrían que actualizar el software para poder utilizar Bitcoin. Por consiguiente, los desarrolladores de Bitcoin y las mayores piscinas de mineros llegaron al acuerdo de seguir con la cadena 0.7, apagando sus servidores degradándolos a la versión 0.7 y volviendo a operar. Finalmente, el aumento del poder computacional de la 0.7 supuso el desarrollo de esta cadena y la resolución de la bifurcación.

- **Abril, 2013:** se produce una burbuja y un crash en las cotizaciones de Bitcoin como se podrá ver más adelante con la explicación de las cotizaciones.

- **Mayo, 2013:** aparece el **primer** servidor ATM o **cajero automático** de BTC. Por otro lado, en este mes se producen dos problemas. En primer lugar, **Bitcoin Central** es

hackeado y pocos cientos de BTC son robados. Bitcoin Central informa a sus usuarios de que no mantengan contacto por el momento y la página pasa a estar en mantenimiento. Las pérdidas son cubiertas por la compañía.

Además, el Departamento de Seguridad de la Patria de los **Estados Unidos incauta** $2.9 millones a una subsidiaria de **Mt.Gox** por violar la regulación en cuanto a transacciones de dinero. Dwolla, la subsidiaria, transfería dinero desde los Estados Unidos a Mt.Gox para comprar y vender BTC. La incautación proviene del fallo en el registro de esta compañía que no figuraba como un negocio de transmisión de dinero. Bitcoin es una divisa descentralizada cuyas principales características están basadas en no estar controlada por un gobierno o banco, con este hecho se pone de manifiesto que, a pesar del funcionamiento del sistema, la regulación y poder de estos organismos son factores que pueden afectar a Bitcoin.

- **Agosto, 2013:** el interés por Bitcoin empieza a acrecentarse con una sucesión de hechos. En el caso contra Trendon Shavers (autor del esquema Ponzi de Bitcoin Savings & Trust), un **juez federal** americano **declara a Bitcoin como dinero real**, ante los intentos del acusado de defenderse alegando que el Bitcoin no es dinero y, por ello, no debería estar perseguido.

Además, **Bloomberg**, la conocida empresa encargada de software financiero, pone a disposición de los usuarios de su terminal un **ticker de Bitcoin**. Un ticker es un símbolo que abrevia un concepto financiero para su identificación. En consecuencia, los usuarios de esta plataforma pueden seguir el desarrollo de Bitcoin y sus datos a través del ticker XBT Currency.

En este mismo mes, el Departamento de Servicios Financieros de Nueva York **(NYSDSF)** emite una **citación a los 22 principales representantes** (compañías y personas) de la red **Bitcoin** para investigar el posible uso de BTC en actividades ilícitas y determinar la necesidad de regulación. Respondiendo también a las quejas de los consumidores acerca de la seguridad de sus fondos. Hay que tener en cuenta que en caso de no existir otra entidad reguladora, este organismo tiene autoridad para regular.

Finalmente, el **ministro de finanzas alemán** confirma que el **Bitcoin** ha sido **reconocido** en el país como un tipo de **dinero privado o "unidad de cuenta"**. Por consiguiente, se puede seguir usando en operaciones comerciales y ventas privadas, está sujeto a impuestos en el caso de mantenerse por menos de un año y, está considerado legalmente como una moneda regional (no llegando a estar al mismo nivel del euro).

- **Octubre, 2013:** tres acontecimientos son relevantes en este periodo. En primer lugar, el **FBI cierra Silk Road**, arrestando al propietario y requisando $3.6 millones en BTC. Este suceso tendrá consecuencias en la cotización como se podrá observar después.

En segundo lugar, **Baidu**, el buscador web más grande de china ("el Google chino"), empieza a **aceptar Bitcoin**. Sin embargo, la adopción de Bitcoin no es en toda la

compañía, sino sólo en el servicio de protección. Este suceso provocará una gran demanda china de bitcoins.

Por último, **BitMarket.eu**, uno de los mayores intercambiadores de BTC, **cierra** por razones de financiación y recursos limitados, lo que no permite atender adecuadamente al incremento de la actividad de la red. (http://bitmarket.eu)

- **Diciembre, 2013:** se produce un gran **robo** de BTC por una suma de 96.000 de **Sheep Marketplace**. Este sitio web operaba como Silk Road, es decir, era un sitio de venta online de droga, el robo provoca el cierre de sus operaciones. Lo curioso de este incidente es que el ladrón comienza a ser perseguido por dos usuarios que aprovechan el historial de transacciones público para rastrear el robo.

Es interesante también un mecanismo que se utiliza para el blanqueo de dinero, Bitcoin Fog, que sirve para barajar los BTC entre numerosas cuentas (juntando BTC de varios usuarios) y, por consiguiente, conseguir desligar los depósitos y extracciones una vez se ha utilizado este servicio, de tal forma que sea imposible relacionar las transacciones y sus usuarios. A pesar de utilizar Bitcoin Fog, una dirección relacionada con el ladrón llegó a albergar 220.000 BTC (toda la información pública puede ser consultada en blockchain.info en todo momento), suma fácilmente reconocible. Se puede advertir los diversos mecanismos que se ofrecen en internet que complementan el uso de Bitcoin, aunque no siempre de una manera honesta.

El **evento más importante** de la historia de Bitcoin ocurre este mes con la **prohibición del Banco Central Chino del Bitcoin**. El Banco Central Chino prohíbe a las instituciones financieras y compañías de pago operar o manejar transacciones con bitcoins, diciendo que **no es dinero con un significado real** y, por tanto, no puede tener la misma legalidad**.** Sin embargo, los individuos pueden comerciar con bitcoins asumiendo el riesgo por ellos mismos. China era uno de los mayores comerciantes de bitcoins hasta la fecha, esta prohibición claramente se verá reflejada en la cotización. Consecuentemente a este suceso, **Baidu deja de aceptar bitcoins**.

- **Febrero, 2014: Mt.Gox**, el intercambiador más importante de Bitcoin, **quiebra** y **cierra.** La compañía es insolvente y declara en el proceso de bancarrota que se debe a la pérdida de 850.000 BTC (750.000 de usuarios y 100.000 de la compañía) por valor de $470 millones aproximadamente) a manos de los hacker. Supuestamente, el robo de 750.000 BTC no fue detectado durante años y, una vez descubierto, produce la insolvencia de la compañía. Se dice que el problema esencial objeto del hack es la maleabilidad de la transacción y los métodos erróneos por parte de Mt.Gox para su control[4].

4 Popper, N., & Abrams, R. (25 de Febrero de 2014). How a bug in bitcoin led to MtGox's collapse. *New York Times*

4. Bitcoin en datos

A. Cotizaciones

En esta sección se va a hacer un estudio de las cotizaciones de Bitcoin en dólares americanos, explicándose los fenómenos asociados a las bajadas y subidas más relevantes.

Previo al análisis se va a explicar el concepto de burbuja y crash. Una **burbuja financiera** es un fenómeno ocurrente en los mercados bursátiles que consiste en una subida anormal y prolongada del precio, debido a la especulación. Con subida anormal se quiere expresar como el precio se aleja del valor intrínseco o real del activo. Es causada por la especulación ya que compradores empiezan a adquirir el producto con la expectativa de venderlo a mayor precio en el futuro. Conforme aumenta la demanda, el precio se eleva alejándose del verdadero valor del activo. Esta espiral ascendente deriva finalmente en la explosión de la burbuja o **crash**.

El **crash** es un acontecimiento financiero ocurrente cuando el nivel de precios de un activo es elevado, sin una base real que justifique el valor de ese producto. Consiste en la venta masiva del activo, todo el mundo quiere vender y existen pocos compradores lo que deriva en una bajada brusca de los precios.

Una vez entendidos estos conceptos, pasemos a las cotizaciones de Bitcoin. Véase el **gráfico 1.**

Como se puede observar en el gráfico, hasta 2011 las cotizaciones de bitcoins son nimias, siendo el valor de un BTC menor a 1$. En febrero de 2011 se alcanza la paridad con el dólar por un corto espacio de tiempo y se mantienen los niveles de cotización anteriores. Finalmente, se advierte una burbuja financiera en junio de 2011, conocida como La Gran Burbuja de 2011**.** El valor de Bitcoin alcanza un máximo de $32 y, en los cuatro días siguientes, se desploma a $10.

El aumento pronunciado del precio se relaciona con la exposición pública de Bitcoin en los medios de comunicación y prensa. Diversos artículos de reconocidos periódicos y revistas como: Forbes, The Economist o The Times hablan de la criptodivisa. Este hecho atrae a inversores que especulan con el valor de Bitcoin. Como se puede recordar de la historia, se suceden los robos siendo Mt.Gox el principal protagonista, lo que causa el crash de la burbuja y la pérdida de valor de los BTC. El resto del año se produce un descenso más estable llegando a una cotización de $2 y cerrándose con un valor aproximado de $4.

Durante 2012 se observa un aumento ligero y progresivo de la cotización llegando a un valor aproximado de $13 en diciembre. En este mes se abre Bitcoin Central que tiene licencia para operar como un banco, lo que provee de confianza a la divisa. Este suceso se reflejará en el mes que viene, momento en el cual la moneda comienza a aumentar a un ratio mayor que en el año 2012.

En el año 2013, el valor de Bitcoin empieza a incrementarse con velocidad alcanzando su punto álgido de $266 en abril. Esta nueva burbuja empieza a fraguarse en el mes de marzo con el rápido incremento de la cotización. Se asocia a este aumento tres eventos:

Primeramente, la regulación de Bitcoin por parte de FinCEN que aporta un marco legal para la actuación de la divisa y, por consiguiente, mayor confianza para los inversores. Y finalmente, la caída económica española y la crisis bancaria de Chipre.

Por un lado, la crisis financiera provoca una caída general de la economía de España durante varios años, lo que supone una mayor desconfianza en el sistema bancario y en los gobiernos. En el mes de marzo se observa un incremento considerable de las descargas del software de Bitcoin ya que supone una posible alternativa al sistema y el estrés financiero.

Por otro lado, el corralito en Chipre de marzo 2013, se bloquea la libre disposición de fondos y se cierran las oficinas bancarias para evitar la retirada masiva de dinero ante un gravamen impuesto por la UE, este gravamen sería parte de un pacto para el rescate del país. Esta situación genera desconfianza de los ciudadanos en el sistema bancario y eleva el interés en Bitcoin.

Como se iba diciendo, este incremento de las cotizaciones alcanza su máximo en abril, momento en el cual se produce el crash. Mt.Gox el intercambiador más importante de la red, con el manejo de un 60% de las transacciones, colapsa. El aumento de tráfico web y de las transacciones provoca lag en los servidores de la compañía (el lag es el tiempo entre que se efectúa una orden por parte de un cliente y es procesada por parte de la empresa). Posteriormente, los clientes no podían acceder a la página web de Mt.Gox porque se encontraba en mantenimiento debido al intenso volumen de comercio. Todos estos pormenores derivan en el pánico y la venta acelerada de Bitcoin.

El declive en el precio continúa y Mt.Gox es víctima de un ataque DDoS lo que obliga al cierre de la página y cese de las transacciones. Un ataque DDoS o ataque de denegación de servicio consiste en la saturación de un servidor que se traduce en que el servicio no sea accesible a los usuarios legítimos. Mediante la emisión de gran cantidad de órdenes de pequeño tamaño se sobrecarga el servidor de Mt.Gox, con el objetivo de un crash con vistas a un beneficio comprando a menor valor y vendiendo cuando se recupere el precio.

La caída en las cotizaciones llega a los $76. Tras una serie de rebotes y la desaparición del pánico financiero el precio se estabiliza aproximadamente alrededor de los $100.

Posteriormente, en otoño el precio incrementa y se consolida en los $130. Si se consulta la gráfica se puede observar una última bajada previa al gran aumento en la cotización. Este pequeño declive se produce en octubre con el cierre de Silk Road (mercado negro de drogas) aunque la recuperación del valor es rápida. Esta recuperación asienta las bases para el crecimiento que se va a analizar ahora, la perdida de los BTC de Silk Road y la estabilización de la cotización supone un indicio para los inversores y una muestra de confianza, ya que se ve que el valor de Bitcoin no depende de las actividades ilegales que se desarrollan en su red (muchas críticas hacían referencia a este hecho).

Junto con el cierre de Bitcoin se produce un evento muy relevante que nos permitirá explicar la subida de la cotización ocurrida en noviembre llegando al máximo valor de Bitcoin en toda su historia. Baidu empieza a aceptar bitcoins lo que supone un aumento de interés chino en la criptodivisa, el intercambiador BTC China releva a Mt.Gox como el mayor intercambiador de bitcoins en volumen de transacciones.

El interés chino por Bitcoin junto con una audiencia del senado estadounidense sobre las divisas virtuales, potencia la publicidad sobre la moneda lo que supone un aumento de la demanda de bitcoins y un crecimiento de la cotización acelerado hasta alcanzar el máximo de $1.240. El mayor conocimiento del concepto supone el aumento de fondos a start-ups y negocios emprendedores relacionados con Bitcoin.

Tras la atención mediática que eleva las cotizaciones hasta máximos históricos se produce el crash. El Banco Central Chino anuncia la prohibición de bitcoins y Baidu deja de aceptar pagos, lo que provoca el desplome de la cotización en un 50% llegando a los $570. La recuperación estabiliza la cotización durante un breve periodo alrededor de los $800.

Después de la estabilización en el precio se observan dos caídas más. En enero de 2014 se produce la detención de Charlie Shrem, CEO de BitInstan y Vice-presidente de The Bitcoin Foundation, bajo la acusación de blanqueo de dinero (venta de bitcoins a Silk Road) y operar sin licencia de negocio transmisor de dinero. Charlie Shrem era una de las personalidades más conocidas en la comunidad Bitcoin y uno de sus líderes más destacados. La noticia supone un descenso de la cotización hasta los $520.

Por último, el valor de los bitcoins vuelve a aumentar hasta el mes de febrero ($670). En febrero varios ataques informáticos a las compañías de intercambio suponen un parón en la retirada de fondos. Estos ataques derivan en el colapso de Mt.Gox y su proceso de bancarrota. Estos eventos originan un derrumbamiento en la cotización de BTC, posicionándose en un valor de $400. Finalmente, tras la recuperación de esta caída se produce un incremento hasta la fecha actual del valor de los BTC, siendo su valor aproximado a junio de 2014 de 650$.

La conclusión que se puede extraer de este histórico de las cotizaciones, es cómo la atención mediática afecta, en gran medida, a un concepto alternativo y experimental como Bitcoin. A su vez, se puede observar la enorme volatilidad a la que está sujeta la criptodivisa por ahora, lo que lleva a la pregunta de si llegará a estabilizarse en el largo plazo.

B. Crecimiento red Bitcoin

En este apartado se quiere mostrar el crecimiento de Bitcoin a partir de la gráfica de **transacciones**, que nos determinará su **uso**, y de la **tasa de hash**, que delimita el **crecimiento computacional** en la red.

En el **gráfico 2** se puede observar el número de transacciones diarias que se realiza con bitcoins a lo largo de la historia. Si se compara con el gráfico 1 se puede advertir que sigue un patrón de crecimiento similar a la cotización, esto es, cuanto más conocimiento sobre el concepto, mayores adeptos que realizan transacciones y ven algún uso en Bitcoin.

Las transacciones se han desarrollado enormemente desde su origen, pasando de 8.000 diarias en mayo de 2012 al rango actual de 50.000 – 70.000 transacciones al día. Actualmente, en términos de utilización, se estima que Bitcoin es el décimo sistema de pago en cuanto a volumen de transacciones, con un valor de $64.474.032[5]. Para que esta valoración tenga un mayor significado, comparémosla con los principales agentes en la red de pagos.

Visa, Inc tiene un volumen aproximado de $16.518.000.000, posicionándose como el primer sistema de pagos utilizado a nivel mundial. En segundo lugar se encuentra MasterCard Inc, con un volumen de transacciones de $9.863.000.000. Vistos estos datos, se deduce que el flujo de operaciones derivado del uso de estas tarjetas de crédito y débito es muy superior al de Bitcoin. Esta diferencia es muy relevante, ya que el principal futuro que se prevé para Bitcoin tiene que ver con los beneficios que ofrece como sistema de pagos online.

---

5 Coinometrics 2014. *Coinometrics*. Recuperado el Junio de 2014, de http://www.coinometrics.com/bitcoin/tix

Por último, en el **gráfico 3** se encuentra la evolución de la tasa hash. Se mide en gigahashes por segundo (miles de millones de hashes) que la red Bitcoin procesa. Este gráfico nos ofrece el desarrollo de la potencia computacional de la red. De nuevo se ve la relación entre el aumento del valor de la cotización y el aumento del poder computacional que se pone al servicio de la minería. A partir del incremento de la cotización de noviembre, más personas quieren ser partícipes de la red Bitcoin. Una de las formas de obtención de bitcoins es a través de la minería, lo que explica este aumento.

Los altibajos de la tasa hash se explican por la dificultad, véase el **gráfico 4**. Al aumentar la capacidad de la red, la dificultad aumenta para mantener el ratio de un bloque cada 10 minutos. Debido a este incremento, usuarios dejan la minería por el problema que supone conseguir la recompensa en un contexto tan competitivo. La dificultad es escalonada porque se ajusta cada dos semanas en función de la velocidad de procesamiento de hashes.

En conclusión, en esta sección se pone de manifiesto el crecimiento de Bitcoin relacionado con el aumento de la cotización. Al elevarse el valor de los bitcoins, aparecen nuevos inversores, mineros y usuarios del protocolo Bitcoin. Todo ello se traduce en un aumento de las transacciones y del poder computacional.

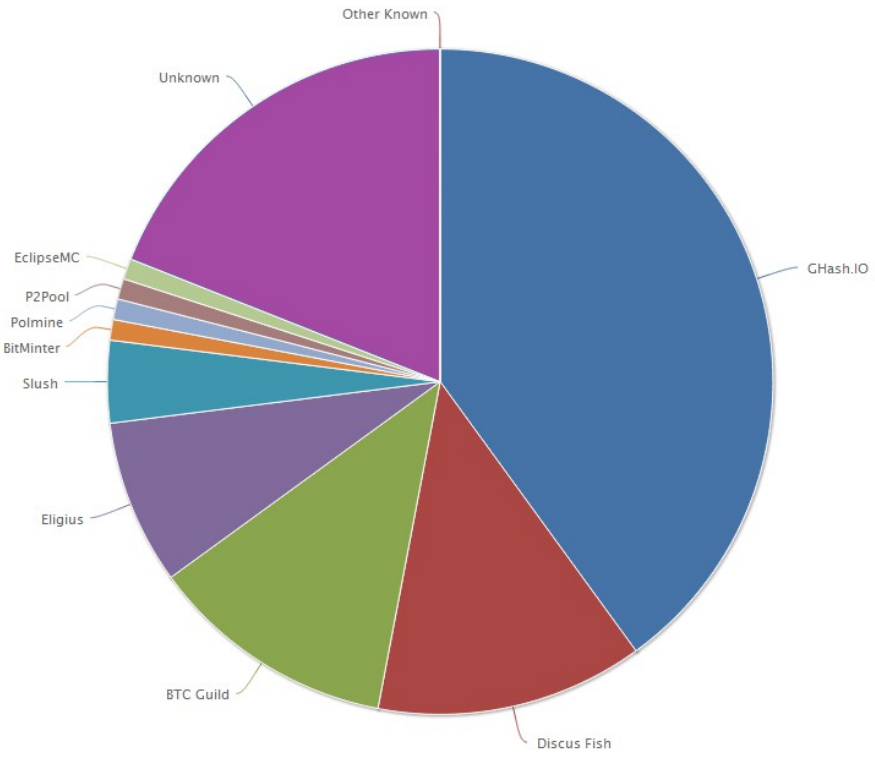
Para comprender hasta qué punto ha crecido la red Bitcoin se ofrece el siguiente dato. Se calcula que el poder de procesamiento de todos los ordenadores del protocolo utilizados en la minería, es de seis veces a ocho veces superior que el top de 500 supercomputadoras mundiales combinadas. Lo cual nos induce a pensar en la utilidad que tendría esta capacidad si se pusiera al servicio de la resolución de problemas más importantes para la humanidad, como curar enfermedades o solventar problemas de futuro[6].

C. Distribución de la tasa hash

Relacionado con el apartado anterior y la tasa de hash, se ofrece un gráfico de tarta[7] para observar la distribución de la minería actualmente.

6 Archer, P. (2013). Bitcoin Network Speed 8 Times Faster than Top 500 Supercomputers Combined.

7 *Blockchain*. Recuperado el Junio de 2014, de https://blockchain.info

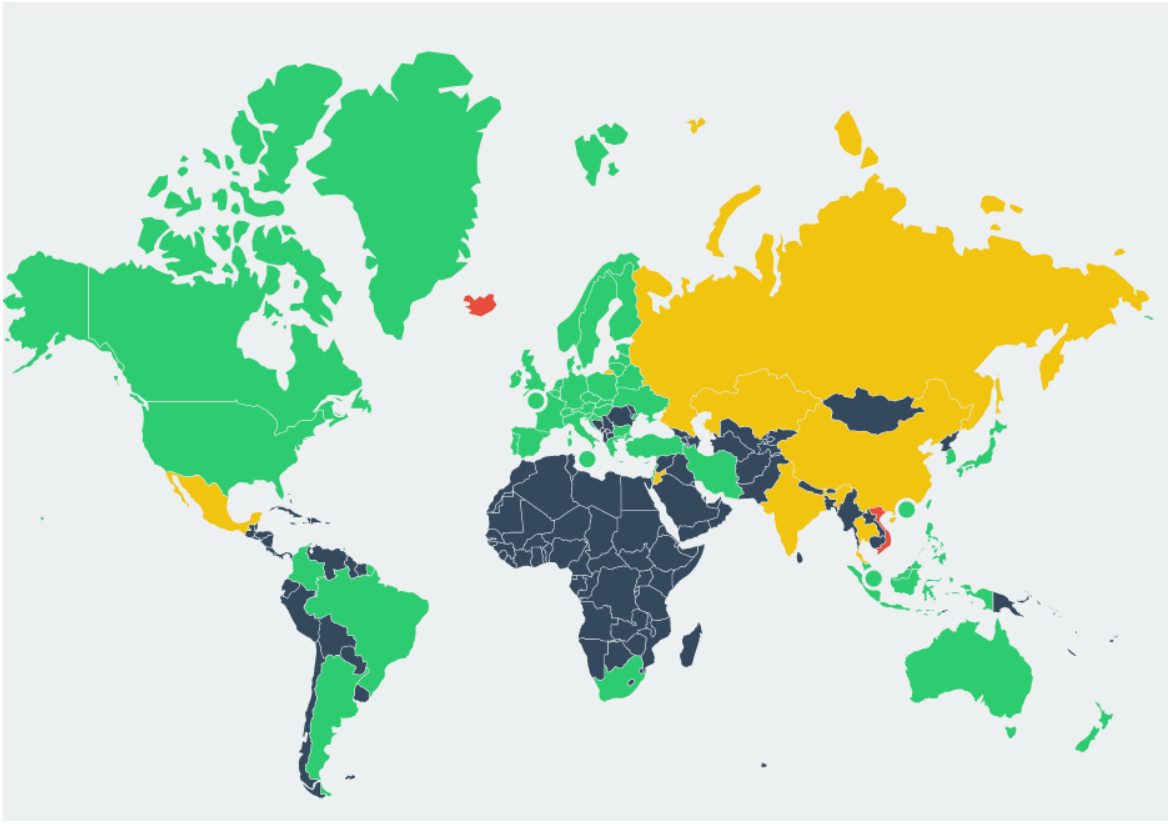


Se puede ver que GHash.IO es la principal piscina de mineros en el mercado con un 40% del poder computacional de la red. Este 40% levanta alarmas con lo referente a un posible control del 51% de la red, que permitiría modificar la cadena de bloques permanentemente y efectuar el doble gasto. Si bien, la propia piscina diluye su poder computacional para no llegar a esa cifra por la preocupación que eso supondría y, a su vez, en el caso de obtener ese porcentaje de control, no saldría rentable malversar y operar maliciosamente ya que la destrucción de la red Bitcoin supondría la pérdida de la inversión en hardware y software minero.

Los mineros desconocidos supondrían el 19% de la red y la siguiente piscina sería Discus Fish con un 13%. En este gráfico se advierte la especialización de la minería. En los primeros años los individuos podían minar bloques, pero la expansión del protocolo y la atracción de nuevos usuarios se traducen en el incremento de la dificultad y la necesidad de colaboración.

D. **Legalidad**

En este último apartado se pretende mostrar la posición legal global que se ha adoptado frente al Bitcoin. La regulación es uno de los grandes problemas de Bitcoin, siendo poco claro cómo ha de ser gravado el concepto o como introducirlo en el marco legal. No se ha llegado aún a un consenso en referencia a estos aspectos. Obsérvese el gráfico.



En verde se encuentran los países que permiten operar con Bitcoin; el color amarillo representa los países en los que está en disputa y abierto a debate; el color rojo (Islandia y Vietnam) son los países hostiles a Bitcoin; y, por último, el color azul oscuro son los países en los que es una incógnita la posición adoptada[8].

Como ejemplo de los países en disputa, el importante caso Chino del que venimos hablando. En diciembre China anuncia la prohibición para operar con bitcoins a las instituciones financieras pero las reglas no han sido desarrolladas. Los intercambios de Bitcoin vuelven a operar en enero de 2014, previo registro a través del ministro de industria e información tecnológica. En marzo se anuncia la intención de emitir reglas claras en lo referente a la divisa digital.

Hay que tener en cuenta que los países que aparecen en verde y, por consiguiente, aceptan Bitcoin, podrían cambiar de parecer en el futuro. En la mayoría de ellos, Bitcoin no está contemplado legalmente y simplemente se permite su utilización. La evolución de la regulación y las posiciones que se adopten, serán esenciales para la supervivencia de Bitcoin.

Concluyendo, en un vistazo superficial se puede advertir que la posición actual de Bitcoin en cuanto a la legalidad no es desventajosa. Economías fuertes como la europea, americana, japonesa y Brasil (emergente) permiten su uso por ahora. Y en el

8 Taylor, Z., Nickel, M., & Brokaw, A. (s.f.). *Bit Legal*. Recuperado el Junio de 2014, de http://bitlegal.io

caso de las economías asiáticas se ha tomado una posición más proactiva en búsqueda de la regulación y, por ello, se genera el debate. Sin embargo, hay que observar cómo se desarrolla la situación legal, ya que tendrá gran importancia en la cotización y futuro de Bitcoin.

5. Viabilidad como moneda

En este punto se va a analizar si Bitcoin cumple las funciones económicas clásicas asociadas al dinero y, por tanto, puede ser considerado como tal. Para ello, se estudiará el comportamiento de Bitcoin como medio de intercambio, unidad de cuenta y almacén de valor.

La primera función, **medio de intercambio**, se refiere a su utilización como intermediario en una transacción de bienes y servicios. En vez de recurrir al trueque con sus claros inconvenientes, se usa el dinero. De esta forma las preferencias del consumidor no influyen en el intercambio de bienes, ya que éstos están evaluados en términos monetarios únicos.

Para que un medio de intercambio sea ampliamente aceptable, ha de conservar un poder de adquisición estable y no mucha volatilidad (cambios en su valor). Bitcoin presenta una gran volatilidad (se estudiará en la parte de almacén de valor) lo que limita su uso como medio de intercambio. Si existe incertidumbre constante acerca del valor que tendrá en el futuro, una persona no puede hacer previsiones respecto al coste de los productos que necesita. En una moneda centralizada el banco y el gobierno aseguran la estabilidad de valor del dinero mediante la implementación de diversas políticas.

No obstante, dado que Bitcoin es un concepto relativamente nuevo y experimental, es razonable que presente gran volatilidad en sus inicios y pueda tender a estabilizarse. Sin embargo, la oferta limitada de bitcoins hace que el valor dependa de la libre demanda del mercado, cuanta más demanda, más valor y viceversa. Con lo que, al carecer de una autoridad que regule el precio y dejarlo a las fuerzas del mercado, los bitcoins son proclives a la volatilidad. Defensores de Bitcoin consideran que una solución plausible sería la programación de los precios de los bienes y servicios para que fluctúen con el valor del Bitcoin. Si bien esto puede ser sencillo mediante el uso de ordenadores, presentaría un entorno turbulento para los consumidores.

Además de este problema de volatilidad, Bitcoin presenta otra desventaja como medio de intercambio. Como cualquier moneda, los bitcoins tienen valor siempre y cuando se acepte como medio de intercambio válido entre dos personas. En este contexto, la aceptación de bitcoins actualmente no es elevada, siendo la mayoría de las transacciones entre inversores con objetivos especulativos. Por consiguiente, si la mayoría de los comercios no acepta BTC, la oferta de productos a la que se puede acceder es limitada. En el futuro podría incrementarse la aceptación de bitcoins con una regulación y conocimiento del protocolo. Sin embargo, el uso de bitcoins requiere ciertos conocimientos informáticos o la confianza en un tercer agente que gestione la seguridad del monedero (trabajo de investigación), lo que limita la amplitud de su uso.

Por último, hay que tener en cuenta el poder de los gobiernos en la utilización del dinero. No pueden modificar el protocolo o afectarlo sin el 51% de la capacidad computacional de la red, pero pueden vetar su uso y utilización a las instituciones dependientes del estado y, sobre todo, nunca podría ser una alternativa factible al sistema monetario, si el gobierno no acepta los bitcoins para el pago de impuestos. Es decir, si el gobierno exige el pago en euros de los impuestos, hay que pagar con euros y los bitcoins tienen valor si se pueden intercambiar por esos euros.

La segunda función es la **unidad de cuenta**, esto quiere decir que el dinero tiene que servir como estándar o medida del valor y el coste de los bienes y servicios. Esto es, se fijan los precios de los productos en función de las unidades monetarias, lo que permite la comparación y evaluación de las diversas posibilidades. Por ejemplo, si una camiseta “x” cuesta 15€ y una camiseta “y” 30€, el precio tiene un significado fácil de inferir, la camiseta “y” cuesta el doble que la camiseta “x”.

Si la economía se estableciera en bitcoins, debido a su volatilidad, los precios de los bienes y servicios tendrían que ajustarse continuamente. La conclusión es que puede ser costoso para los comercios y confuso para los consumidores. Además, si analizamos el entorno actual, podemos observar que el valor de un BTC es muy elevado, lo que haría que productos de bajo coste presentaran números difíciles de evaluar y comparar. Por ejemplo, una barra de pan podría costar 0.0058 BTC y un paquete de chicles 0.000132 BTC. Claramente estos números ofrecen una dificultad de cálculo adicional a la hora de comparar alternativas y no suponen un punto de referencia para un consumidor medio.

Finalmente, hay que tener en cuenta el precio actual de los bitcoins en el mercado. En este mismo momento, se pueden encontrar bitcoins a $642.77, $626.50 y $627.113[9] en diferentes casas de cambio. Esta diversidad de precios va en contra de la ley de un solo precio y permite acciones de arbitraje, esto es, comprar a $626.50 en una casa de cambio y vender a $642.77 en la otra, obteniendo un beneficio con la compraventa. Esta es una nueva muestra de la incertidumbre del valor de Bitcoin incluso entre casas de cambio.

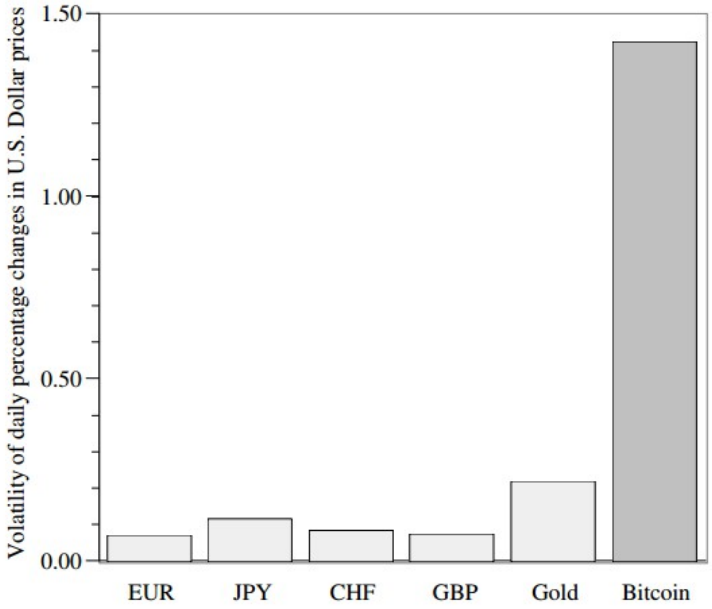
La tercera y última función de estudio es el **almacén de valor[10]**, se refiere a que un activo pueda guardarse, recuperarse e intercambiarse en el futuro, de manera que sea predecible la utilidad del activo una vez recobrado. En definitiva, que el dinero tenga un valor estable, permitiendo que la moneda se obtenga en un momento determinado y se pueda cambiar posteriormente por bienes y servicios.

En este contexto Bitcoin presenta dos grandes inconvenientes. Por un lado, al guardarse la divisa se hace frente a los problemas de seguridad informáticos, si no se es precavido con los fondos estos pueden ser robados. Un usuario medio tendría que informarse del funcionamiento del Bitcoin y pensar métodos adecuados para su protección, o confiar sus fondos a una compañía de gestión de monederos online. Sin embargo, en la evolución de Bitcoin se puede observar como las vulnerabilidades son aprovechadas por cibercriminales, haciendo necesario una investigación previa de la institución en la que se depositan los fondos.

Por otro lado, el eterno problema de la volatilidad. Mantener bitcoins actualmente conlleva un gran riesgo, ya que no se sabe el valor que adoptará en el futuro. Obsérvese la gráfica siguiente:

9 *Bitcoin Charts*. Recuperado el Junio de 2014, de http://bitcoincharts.com/

10Krugman, P. (28 de Diciembre de 2013). Bitcoin is evil. *New York Times* .



Esta gráfica[11] presenta la enorme volatilidad de Bitcoin. Esta calculada utilizando los datos diarios de 2013 anualizados, del ratio de intercambio con el dólar americano. Y se compara con la volatilidad del euro, el yen japonés, el franco suizo, la libra británica y el oro. Como se puede ver la volatilidad de Bitcoin es cuantiosa, 142%, lo que limita su uso como moneda y demuestra la especulación subyacente.

En conclusión, se puede observar la poca estabilidad de Bitcoin como medio de almacenamiento de valor. En una divisa como el euro, se extrae que el valor proviene del respaldo de un banco y un gobierno. Se pueden utilizar euros para pagar los impuestos al gobierno y, en caso de una disminución del valor real del dinero, el banco seguiría aceptando esos euros.

En Bitcoin no existen estas entidades, el valor se determina en función de una demanda errática e incierta. Por consiguiente, tras el razonamiento expresado, se concluye que Bitcoin no puede ser reconocido actualmente como moneda y no es, en este momento, una alternativa realista al sistema monetario. Si en el futuro se estabiliza el valor de los bitcoins, podría estudiarse su factibilidad económica en concepto de moneda.

11 Yermack, D. (1 de Abril de 2014). Is bitcoin a real currency?

6. Análisis DAFO

En esta sección se realizara un análisis DAFO de la criptodivisa. Este análisis nos permitirá entender la situación actual de Bitcoin a través de dos puntos: su situación interna (Fortalezas y Debilidades) y su situación externa (Oportunidades y Amenazas).

Fortalezas

i. **Arquitectura descentralizada:** la información es gestionada por los usuarios y no depende de la confianza y control de una autoridad central. Permite a Bitcoin funcionar como una plataforma de pago abierta e independiente. Además, tiene una estructura democrática, de manera que siempre que el 51% de la red sea honesta, ningún usuario podrá saltarse las normas establecidas en el protocolo.

ii. **Criptografía:** el sistema criptográfico en el que se sustenta es fuerte y su efectividad está probada, si las técnicas se utilizan correctamente el almacenamiento de bitcoins es seguro. Si bien, podría quedar obsoleto en el futuro con el avance de los algoritmos matemáticos. Sin embargo, el protocolo permite su modificación mediante el consenso entre sus usuarios. Siempre y cuando se mantenga actualizado, no debería suponer un problema.

iii. **Anonimato:** este punto supone también una debilidad dependiendo del punto de vista. Es una fortaleza porque ofrece la posibilidad de realizar transacciones sin el control y rastreo de un tercer agente. Además, imposibilita la congelación de fondos permitiendo la libre disposición de los mismos en todo momento.

iv. **Transparencia:** a pesar de permitir el anonimato, Bitcoin es una plataforma de pagos totalmente transparente, toda la información de las transacciones está disponible en la cadena de bloques. Este hecho permite rastrear actividades ilícitas (caso de SheepMarket en la evolución) y otras transacciones (lo cual supone una debilidad también).

v. **Bajas comisiones:** al no existir intermediarios en una transacción, los costes por este servicio desaparecen. Siendo las comisiones voluntarias para acelerar el proceso de confirmación.

vi. **Internacional y rápido:** las transferencias de dinero a nivel internacional son más veloces que si se realizarán a través de otras plataformas. En los sistemas tradicionales, pueden tardar en completarse un día o más. En el caso de España por ejemplo, la regulación impone un día hábil para la ejecución de estas órdenes.

vii. **Incentivos:** el sistema de incentivos creado para el protocolo Bitcoin es una genialidad que permite crear unidades monetarias y conseguir el poder computacional que sustente la red.

viii. **Innovación:** el protocolo supone una gran innovación tecnológica, siendo la primera divisa digital que soluciona el problema del doble gasto sin requerir a una tercera parte involucrada en una transacción.

ix. **Disponibilidad de intercambio con monedas convencionales:** se pueden intercambiar BTC por divisas ampliamente aceptadas.

Debilidades

i. **Descentralización:** supone una debilidad ya que la ausencia de un agente central dificulta la adaptación a los cambios del mercado y mina la confianza en el sistema.

ii. **Vulnerabilidades:** a pesar de gozar de una fuerte criptografía, la mala implementación de sus técnicas se traduce en brechas de seguridad que pueden aprovechar usuarios maliciosos. A lo largo de la evolución de Bitcoin hemos podido observar estos fallos en el sistema. También supone una desventaja por el conocimiento informático necesario para mantener los fondos seguros, lo que hace que un usuario medio sea reticente a su aceptación (o necesita de un tercer agente en el que depositar su confianza).

iii. **Aceptación:** su valor depende completamente de la aceptación entre los usuarios como medio de pago, sin el respaldo de ningún banco o gobierno. Actualmente Bitcoin es percibido como un activo de especulación como veíamos anteriormente.

iv. **Transparencia:** la transparencia de las transacciones se postula también como un inconveniente, ya que el acceso de los usuarios a toda la información de la red implica que sean necesarias medidas de seguridad complementarias para salvaguardar los fondos.

v. **Anonimato:** presenta dos problemas fundamentales. Relacionado con el punto anterior, la integridad y privacidad de un usuario puede ser vulnerada, una vez se consigue una identidad (queda comprometida por diversas razones, técnicas informáticas o mala gestión del usuario), se puede saber en todo momento la cantidad de fondos de los que se dispone y la gestión de los mismos. Este riesgo añade una complicación, la necesidad de una gestión efectiva de las direcciones Bitcoin. Además, la operación a través de pseudónimos permite el comercio ilegal y el blanqueo de dinero. Todo ello sujeto, como en el caso de los usuarios, a un buen control informático.

vi. **Volatilidad:** es una desventaja desde cualquier perspectiva con excepción de la especulativa. Como veíamos, la volatilidad impide que los bitcoins puedan ser considerados moneda, ya que no cumple con los requisitos funcionales de la economía. Supone un riesgo constante para la conservación de bitcoins, debido a la incertidumbre en lo referente a su valor futuro.

vii. **Consumo de energía:** la minería requiere de un constante gasto en electricidad para mantener los ordenadores operativos. El aumento de la dificultad en la prueba de trabajo, la reducción de las recompensas y el coste de la electricidad, podría hacer que a largo plazo no resultará rentable realizar la actividad de la

minería. Se podría paliar este inconveniente con el aumento de las comisiones de transacción.

viii. **Tendencia deflacionaria:** la oferta monetaria limitada implica que los bitcoins tienen tendencia deflacionaria. Esto es negativo porque la apreciación constante de la divisa incita al ahorro, lo cual en sí mismo no es problemático, pero deriva en la reducción del flujo monetario presente en la economía. Si la demanda se reduce, los comercios tienen que reducir sus costes, la plantilla se recorta, más parados supone menos demanda y, así sucesivamente, produciendo un estancamiento en la economía.

ix. **Código abierto:** supone una gran ventaja en el sentido que provee confianza al protocolo, todo el mundo puede consultar su funcionamiento. Pero es una debilidad, económicamente hablando, porque favorece una gran competencia (como es el caso), cualquiera puede consultar el código y modificarlo mínimamente proveyendo un servicio similar. La competitividad será analizada más cuidadosamente en las amenazas.

Oportunidades

i. **Moneda alternativa:** en el análisis previo concluíamos que Bitcoin es poco realista que sustituya a las monedas actuales. Sin embargo, es posible que adquiera cuota de mercado si su valor se estabiliza en el futuro. Muchos de los adoptantes de Bitcoin confían en que pueda ser una opción viable, pero la ausencia de una autoridad central que ayude a controlar el precio de BTC y ofrezca respaldo a la divisa, mina la confianza y la utilidad de este sistema. A todo ello, se le junta la necesidad de conocimientos informáticos, que impiden su adopción general por la sociedad.

ii. **Plataforma de pagos:** sin duda esta es la mayor oportunidad que se le presenta a Bitcoin. La concepción del protocolo permite transferencias rápidas y sin comisiones entre sus usuarios. Supone una innovación tecnológica en el sistema tradicional de pago online, los principales agentes no ofrecen las mismas características beneficiosas de pago. En este contexto, tarjetas de crédito y compañías como PayPal, están sujetas a importantes comisiones y, en el caso de las transferencias bancarias, a las comisiones se les añade el tiempo que tarda en hacerse efectiva la orden.

iii. **Especulación:** la oferta limitada de bitcoins implica que si el número de usuarios aumenta en el largo plazo, el valor subirá pudiéndose aprovechar esta característica con motivos de inversión. Esta oportunidad se presenta de cara un inversor y no para el sistema Bitcoin en sí. Hay que tener en cuenta el riesgo que presenta su volatilidad en cualquier caso.

iv. **Internacionalización y gran mercado:** Bitcoin está diseñado para permitir transacciones a través de internet, lo que hace que el mercado al que está dirigido sea internacional y muy amplio. Esto supone que cualquier persona en el planeta puede ser un usuario potencial del sistema. Es una oportunidad ya que, mientras funcione y sea adoptado en varios países, seguirá aportando valor a sus inversores y usuarios.

Amenazas

i. **Ataques informáticos:** como se pudo observar en la evolución de Bitcoin, los agentes e individuos operando en este mercado están sujetos a hacks informáticos. Si bien el protocolo no se ha visto comprometido y la criptografía es segura, un usuario medio no aceptará el concepto si corre el riesgo de perder sus ahorros a manos de un cibercriminal. Esta amenaza es constante, requiriendo una continua actualización y dinamismo por parte de las instituciones a cargo de fondos BTC.

ii. **Legalidad:** Bitcoin es una start-up tecnológica y un nuevo concepto en la sociedad, esto hace que se encuentre en un momento de incertidumbre en cuanto a la regulación y suponga un vacío legal. Por tanto, se corre el riesgo de una regulación desfavorable (Islandia o Vietnam), como previamente se mostraba la situación legal de Bitcoin en el mapamundi. Por otro lado, un marco legal puede ofrecer confianza a los usuarios para su adopción en determinados aspectos. La evolución de este apartado determinará en gran medida el éxito de la criptodivisa.

iii. **Competición:** el código abierto de Bitcoin permite modificaciones ligeras en el protocolo y la creación de criptodivisas alternativas. Desde la solución del problema de doble gasto, han aparecido numerosos competidores en el mercado, entre ellos se puede destacar: Litecoin, Dogecoin, Mastercoin, Peercoin o Darkcoin. Éstos simplemente cambian especificaciones técnicas, como el límite de la oferta monetaria, la velocidad de minado, los ajustes de dificultad o las recompensas. Actualmente no son tan sonados como Bitcoin teniendo una capitalización de mercado muy inferior. Por ejemplo, la cotización de la segunda criptomoneda, Litecoin, es de $10.60[12]. Sin embargo, en el futuro podrían ser una amenaza para el negocio, sobre todo si tenemos en cuenta el carácter estático del protocolo Bitcoin. Una start-up ágil y con una buena idea subyacente podría sobreponerse a los cambios de mercado de manera más efectiva.

iv. **Deflación:** ya se ha explicado este aspecto en otros apartados. Para evitarla, tendría que poder expandirse la oferta monetaria y no estar limitada.

12 CoinMarketCap. Recuperado el Junio de 2014, de https://coinmarketcap.com

7. Conclusión

Se ha analizado el concepto Bitcoin y su evolución. A partir de ellos, se puede comprender el resto de apartados, es decir, los datos, viabilidad como moneda y el análisis DAFO. Las conclusiones que se van a presentar se basan, en especial, en el análisis DAFO y la viabilidad de Bitcoin como moneda.

Se estructurará la conclusión en forma de resumen de todos los puntos estudiados. Bitcoin es una criptodivisa descentralizada de código abierto, supone una gran innovación tecnológica al solventar el problema del doble gasto en internet mediante el uso de la cadena de bloques. La cadena de bloques funciona como un libro mayor contable y los mineros se encargan de proteger la integridad de la misma. Los mineros tienen una serie de incentivos que les llevan a poner al servicio del protocolo su capacidad computacional.

Las recompensas por la creación de bloques son la forma de introducir nuevas unidades monetarias en el sistema. La oferta monetaria está limitada a 21 millones, lo que se traduce en una tendencia deflacionaria muy criticada por los economistas.

Bitcoin ha evolucionado con rapidez, en gran medida se puede explicar por la crisis financiera acaecida que produce desconfianza en los gobiernos y bancos. La desventaja de este desarrollo es que la mayor atención supone más interés de los cibercriminales en adquirir la divisa, poniendo en peligro la seguridad de los agentes que operan en el mercado. A su vez, atrae a inversores especulativos que mueven el valor de la divisa haciéndola más inestable y volátil.

El precio de mercado de los bitcoins es muy volátil e inestable, existe gran incertidumbre respecto al valor que tomará en el futuro. Los altibajos en la cotización se pueden explicar, en gran parte, por la atención mediática que atrae a inversores y las decisiones de los gobiernos respecto a Bitcoin. También, los fallos y vulnerabilidades afectan a la cotización.

La red de mineros de Bitcoin se ha especializado enormemente en un pequeño número de piscinas de mineros. Esta especialización conlleva un aumento considerable del poder computacional en la red y plantea el riesgo de una piscina obteniendo el 51% de la red y, por tanto, consiguiendo el control de la misma.

Bitcoin se encuentra en la mayor parte del mundo en un momento de vacío legal. Pocas autoridades han tomado una posición proactiva en cuanto a la regulación del sistema y el ofrecimiento de un marco legal. China es el caso más conocido e importante de la historia de Bitcoin.

Se ha observado que Bitcoin no cumple los requisitos básicos económicos para ser considerado moneda. La volatilidad y su carácter informático hacen difícil que en el futuro la criptodivisa pueda suponer una alternativa realista a las monedas convencionales.

El análisis DAFO nos presenta las mayores posibilidades y amenazas a las que tiene acceso y se enfrenta Bitcoin. Su supervivencia estará marcada por como solvente la regulación de los gobiernos, la cuantiosa competencia, los fallos de seguridad y la deflación. Muchos de estos problemas podrían ser solucionados mediante la existencia

de un organismo central que respaldará la divisa y reaccionará con velocidad a los cambios del mercado.

Visto lo visto, la mayor oportunidad que se le presenta a Bitcoin es su utilidad como plataforma de pago online. Como se ha dicho muchas veces, supone una gran innovación la solución del problema del doble gasto (diferenciándose de divisas digitales anteriores), las comisiones de transacción son nimias y goza de velocidad en la transferencia internacional de fondos. Actualmente ocupa el décimo puesto en el ranking de plataformas de pago.

Por consiguiente y concluyendo, considero que Bitcoin no va a sobrevivir en el largo plazo como moneda y puede resultar viable como método de pago online o activo de especulación. Si bien, al ser un concepto experimental se encuentra en una época de gran incertidumbre.

Definitivamente, Bitcoin supone una revolución y un avance tecnológico pero su arquitectura en código abierto permite la imitación y mejora del concepto. Con lo que, en mi opinión y en base a todo lo expresado en esta investigación, creo que Bitcoin no va a aguantar en el largo plazo, pero un concepto similar que solucione los problemas que presenta esta criptodivisa, puede alzarse como una alternativa fuerte a una moneda centralizada y alcanzar el liderazgo como plataforma de pagos.

Bitcoin es un nuevo paso en el entorno dinámico de Internet, en el corto y medio plazo, con una regulación por parte de los gobiernos se determinará hasta qué punto es válida la criptodivisa y si es un competidor capaz de desbancar a las principales plataformas de pago, Visa y MasterCard. Dudo que este último aspecto llegue a buen término por la general aceptación de la que gozan estos sistemas de pago, frente a un concepto complejo y difícil de entender como Bitcoin, que requiere de sus usuarios ciertos conocimientos no habituales en la vida cotidiana.

8. Bibliografía

Antes de presentar la bibliografía quisiera mencionar que los primeros apartados no están sustentados en bases científicas, esto es, el protocolo Bitcoin es de código abierto y cualquier usuario puede consultar el funcionamiento del mismo. Por ello, el

desarrollo de esos puntos se ha realizado mediante la consulta de fuentes de la red Bitcoin, contrastando diversos orígenes y gestionando el resultado por mi cuenta.

A su vez, la evolución de Bitcoin está basada en numerosas noticias que no se citan en el texto por cuestiones de no saturar el documento. Se presentarán a continuación.

Dicho esto, la bibliografía está compuesta por:

- 2009-2014, B. P. *bitcoin.org*. Recuperado el Mayo de 2014, de https://bitcoin.org
- A dream dispelled. (12 de Abril de 2014). *The Economist* .
- A, R. (3 de Abril de 2014). Bitcoin's deflation problem. *The Economist* .
- Archer, P. (2013). Bitcoin Network Speed 8 Times Faster than Top 500 Supercomputers Combined.
- bitcoincharts.com. *Bitcoin Charts*. Recuperado el Junio de 2014, de http://bitcoincharts.com/
- Bitcoinmining. *Bitcoinmining.com*. Recuperado el Mayo de 2014, de http://www.bitcoinmining.com/
- *Block explorer*. Recuperado el Mayo de 2014, de http://blockexplorer.com/
- *Blockchain*. Recuperado el Junio de 2014, de https://blockchain.info
- Boase, R. (2013). Bitcoin Price Skyrockets as Senate Hearing Concludes. *Coindesk* .
- Cawrey, D. (26 de Mayo de 2014). The Five Biggest Threats Facing Bitcoin. *Coindesk* .
- CoinMarketCap. Recuperado el Junio de 2014, de https://coinmarketcap.com/
- Coinometrics, 2. *Coinometrics*. Recuperado el Junio de 2014, de http://www.coinometrics.com/bitcoin/tix
- Crippen, A. (14 de Marzo de 2014). Buffett blasts bitcoin as 'mirage': 'Stay away!'. *cnbc* .
- Goldman Sachs. (11 de Marzo de 2014). Top of Mind.
- Grinberg, R. (9 de Diciembre de 2011). Bitcoin: An Innovative Alternative Digital Currency.

- Hern, A. (27 de Febrero de 2014). How a bug in bitcoin led to MtGox's collapse. *The Guardian* .
- Hill, K. (2014). Bitcoin Battle: Warren Buffett vs. Marc Andreessen. *Forbes* .
- Hill, K. (2013). Bitcoin Valued At $1300 By Bank of America Analysts. *Forbes* .
- Hill, K. (2014). Silk Road Bitcoin On The Move For Government Auction Of $18 Million Worth At End Of The Month. *Forbes* .
- *History of Bitcoin*. Recuperado el Junio de 2014, de http://historyofbitcoin.org/
- Kitko News. (2013). 2013: Year Of The Bitcoin. *Forbes* .
- Kristoufek, L. (2 de Junio de 2014). What are the main drivers of the Bitcoin price?
- Krugman, P. (28 de Diciembre de 2013). Bitcoin is evil. *New York Times* .
- Lee, T. B. (2013). An Illustrated History Of Bitcoin Crashes. *Forbes* .
- Manjoo, F. (5 de Marzo de 2014). For Bitcoin, Secure Future Might Need Oversight. *New York Times* .
- McMillan, R. (2014). The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster. *Wired* .
- Moore, T., & Christin, N. (2013). Beware the Middleman:Empirical Analysis of Bitcoin-Exchange Risk.
- Möser, M. (2013). Anonymity of Bitcoin Transactions.
- Nakamoto, S. (Octubre de 2008). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario* .
- Niemi, R., Abrams, R., & Daniel, J. (4 de Abril de 2014). How to explain Bitcoin to your mom. *New York Times* .
- Popper, N., & Abrams, R. (25 de Febrero de 2014). How a bug in bitcoin led to MtGox's collapse. *New York Times* .
- Rizzo, P. (20 de Marzo de 2014). Saxo Bank CEO: Bitcoin is an Opportunity for Early Adopters. *Coindesk* .
- Steadman, I. (2013). Bitcoin interest spikes in Spain as Cyprus financial crisis grows. *Wired* .

- Taylor, Z., Nickel, M., & Brokaw, A. (s.f.). *Bit Legal*. Recuperado el Junio de 2014, de http://bitlegal.io/about.php
- Wallace, B. (2011). The Rise and Fall of Bitcoin. *Wired* , 4.
- Woo, D., Gordon, I., & Iaralov, V. (2013). *Bitcoin: a first assesstment.*
- Yermack, D. (1 de Abril de 2014). Is bitcoin a real currency? .

9. Anexo: Gráficos

Gráfico 1:

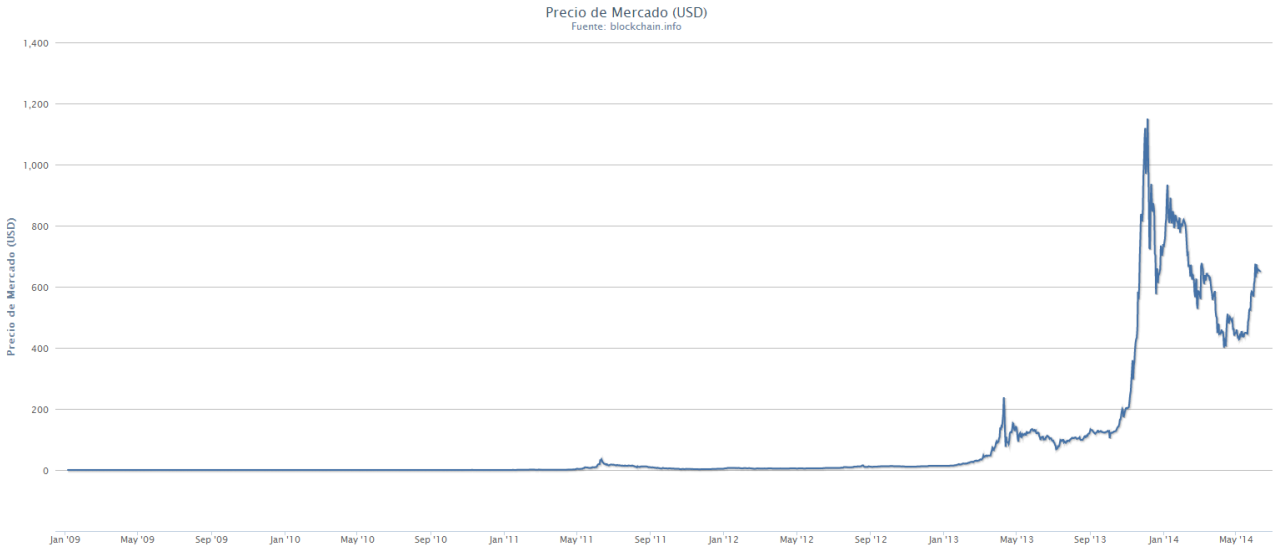


Gráfico 2:

Gráfico 3:


Tasa de Hash
Fuente: blockchain.info
Tasa de hashs en GH/s
110,000,000
100,000,000
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
Jan '09
May '09
Sep '09
Jan '10
May '10
Sep '10
Jan '11
May '11
Sep '11
Jan '12
May '12
Sep '12
Jan '13
May '13
Sep '13
Jan '14
May '14

Gráfico 4:


Dificultad
Fuente: blockchain.info
Dificultad
14,000,000,000
12,000,000,000
10,000,000,000
8,000,000,000
6,000,000,000
4,000,000,000
2,000,000,000
0
Jan '09
May '09
Sep '09
Jan '10
May '10
Sep '10
Jan '11
May '11
Sep '11
Jan '12
May '12
Sep '12
Jan '13
May '13
Sep '13
Jan '14
May '14