Bitcoin

Por Fernando J. Martini corregido por Oscar Castro

El sistema de dinero electrónico denominado Bitcoin nació con la idea de descentralizar los pagos entre usuarios, eliminando la presencia de instituciones financieras en las transacciones. Aunque no exenta de polémica, esta solución ha demostrado, hasta ahora, que funciona.

El 8 de noviembre de2008 apareció un *paper* publicado en el portal *P2P foundatio* bajo el seudónimo de Satoshi Nakamoto (hasta hoy se desconoce su verdadera identidad) denominado "Bitcoin: A Peer-to-Peer Electronic Cash System". Luego de que muchos autores realizaran importantes esfuerzos y contribuciones para la creación de una moneda electrónica, este *paper* parecía aportar lo que faltaba para dar a luz una moneda electrónica (también llamadas criptomoneda). Después de un arduo trabajo de un equipo de programadores liderados por el mismo Satoshi (a quien sólo se lo conocía por las comunicaciones que emitía por la red), el 3 de enero de 2009, se puso en marcha Bitcoin.

1- La moneda que todos conocemos

Mucho es lo que se puede hablar sobre la moneda que de antaño se conoce. Aquí sólo se verterán algunos pocos conceptos sobre la moneda para poder introducirnos al conocimiento del Bitcoin. El papel moneda o una moneda de metal hace referencia a un pedazo de papel o de metal que tiene un valor fiduciario. Fiduciario significa que se basa en la fe y la confianza de la comunidad. Esta fe y confianza se sustenta en que las monedas que se utilizan están emitidas por una autoridad pública confiable que depende de un estado o conjunto de estados asociados. Las típicas monedas se generan en papel o metal con estrictas reglas de seguridad para evitar su falsificación. Los estados que las sustentan tienen una estructura jurídica (o marco legal) que les da confiabilidad. Cuanto más jurídicamente confiable sea el estado o los estados que las emiten más confiable será la moneda generada. Por este motivo, a estas monedas también se las llama monedas de curso legal. Para los estados es de vital importancia la utilización de una moneda de curso legal confiable y son muchas las implicancias que la moneda tiene sobre la economía de los países.

2- La vida cotidiana del dinero cuando los bancos no manejaban las tecnologías de la información

Por ejemplo, una persona recibía el pago del jornal o del sueldo mediante la utilización del papel moneda de curso legal (de ahora en más se obviará la moneda metálica). Este utilizaba el papel moneda para pagar sus necesidades y cuando le quedaba un remanente, en general, lo llevaba personalmente a un banco confiable que se lo guardaba en forma segura. Cuando esta persona, por algún motivo, necesitaba el dinero pasaba por el banco a retirarlo. Por el otro lado, el banco mantenía una simple **cuenta** de cuanto dinero le entregaba el asalariado y de cuanto retiraba. La diferencia de las entradas y las salidas es lo que se conoce como **saldo de la cuenta**. De esta forma aparece una forma de dinero que ya no es papel moneda sino que es un número expresado en moneda de curso legal que el banco tiene anotado en un registro asociado a un cliente. El banco puede o no tener en sus arcas la totalidad del papel moneda recibido. Por regulaciones de los estados, a través de los bancos centrales se establece la cantidad de papel moneda que el banco debe guardar y cual es la cantidad que el banco puede prestar. Esta posibilidad que tienen los bancos de no tener que guardar la totalidad del dinero recibido y poder prestar una parte, genera un aumento de la moneda de curso legal pero que no es papel moneda. Este mecanismo se denomina multiplicador monetario. Para dar un ejemplo:

> Suponiendo que los bancos deben mantener un encaje (que es la cantidad de dinero que el banco no puede prestar) de 30%.
>
> 1- Una persona A deposita en el banco B $ 1.000
> 2- El banco B de esos $ 1.000 presta $ 700 al cliente C.
> 3- El cliente C compra mercadería a un proveedor D con los $ 700 que se le prestaron.
> 4- El proveedor D deposita en el banco B $ 700.
> 5- El banco B presta $ 490 al cliente E.

Ahora la cantidad de moneda de curso legal que originalmente eran $ 1.000 son: los $ 1.000 de A más los $ 700 de D más los $ 490 de E.

En el anterior ejemplo se puede observar que hay dinero que es solo un valor expresado en moneda de curso legal contabilizado en **cuentas** de los bancos. Este dinero es fiduciario ya que también se basa en la confianza que la comunidad tiene sobre los bancos y sobre el sistema jurídico del estado en general.

3- Los bancos y la aparición de la tecnología de la información

Ahora los clientes de los bancos pueden hacer sus pagos transfiriendo dinero de una **cuenta** a otra **cuenta** (del mismo banco o de distintos bancos) utilizando Internet y sin la necesidad de mover papel moneda. Los bancos compensan sus operaciones cruzadas en **cuentas** que todos los bancos deben poseer en el banco central del estado.

También se pueden hacer pagos con tarjetas de débito, que funcionan de una forma muy parecida a una transferencia bancaria, o se pueden hacer pagos con tarjetas de crédito. En este último caso, cuando un vendedor recibe un cobro con tarjeta de crédito el importe vendido se le acredita a fin de mes en su **cuenta** bancaria. El comprador pagará ese dinero a fin de mes con un débito en su **cuenta** o en cuotas mensuales en función de su capacidad crediticia.

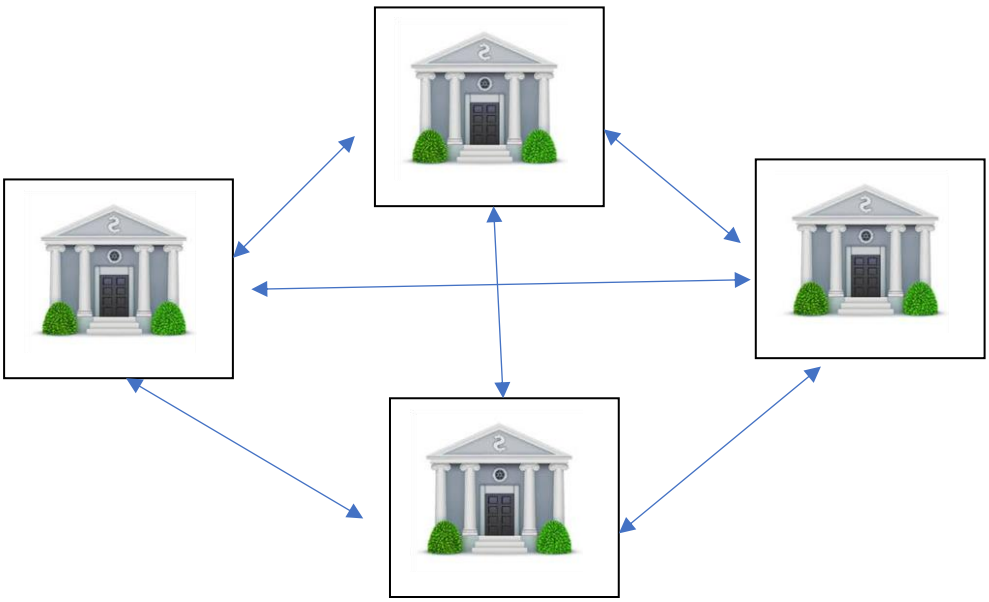
Existen otras formas de pagos, pero que en todos los casos son movimientos de **cuentas** que están referidas a una moneda de curso de legal de algún estado o conjunto de estados.

Estas **cuentas** son simplemente saldos, justificados con movimientos de entras y salidas, que en lugar de estar escritas en un papel, están almacenadas en las bases de datos de los sistemas informáticos. Los bancos tienen estrictos controles sobre estas bases y la forma en que se efectúan las operaciones entre bancos o entre otro tipo de entidades (American Express, PayPal, Dinero Mail, Mercado de Pagos, etc.).

4- Introducción a qué es Bitcoin

Bitcoin es una moneda que existe sólo en **cuentas** digitales. Estas existen en computadoras interconectadas que trabajan bajo un mismo protocolo (o conjunto de normas) establecido por la comunidad de Bitcoin.

Haciendo una analogía, puede verse como un banco con múltiples sucursales interconectadas pero sin casa central.



Todas las sucursales son autónomas pero trabajan bajo un mismo conjunto de normas. Saliendo de la analogía, lo que se representó recién como bancos, son nodos de una red donde cada nodo tiene hardware y software adecuado para participar de la red de Bitcoin. Cualquier persona con una computadora (relativamente potente) y una conexión a Internet puede pasar a ser un nodo de la red. No tiene que pedirle permiso a nadie. Solo tiene que instalar en su computadora el software preciso para la red de Bitcoin. Este software es el que contiene todas las reglas que regulan Bitcoin. La red Bitcoin funciona bien siempre y cuando todos los nodos de la red utilicen software aprobado por Bitcoin. Seguro el lector ya tendrá dudas respecto de ¿quién hace este software? ¿Quién prueba y aprueba el software que todos los nodos de la red utilizan? ¿Quién y cómo se autorizan los cambios? ¿Dónde se puede obtener este software? Más abajo se dará respuestas a estas preguntas, ahora conviene pasar a explicar como está funcionando la red de Bitcoin hoy.

5- Conceptos básicos del funcionamiento de Bitcoin

Bitcoin está diseñado para que su moneda sea divisible en fracciones muy pequeñas. La unidad de medida más pequeña en la que puede dividirse 1 bitcoin (BTC) se llama Satoshi (recuérdese que es el seudónimo de su creador), 1 Satoshi equivale a 0,00000001 bitcoin.

Un BTC comenzó valiendo 0,07 dólares en el 2011, en el año 2017 hubo una burbuja de crecimiento desbocado que llevó el valor a 17.000 dólares. A la fecha de este artículo se está cotizando a 6.460 dólares.

En estos momentos, la cantidad de BTC en el mercado es de aproximadamente 17.200.000 y está estipulado, por software, que alcance la cantidad de BTC 21.000.000. Cuando se llegue a esta cifra no se emitirán más Bitcoin. Los especialistas de Bitcoin estiman que esta cifra se alcanzará, recién, en el año 2140. La forma en la que se incorporan BTC al mercado es por el mecanismo de "minado" que luego se explicará.

Bitcoin es un registro único de transacciones de BTC. Una transacción de bitcoin se forma, básicamente, por entradas y salidas de BTC asociadas a una dirección (algo similar a las **cuentas** de los bancos). La dirección de Bitcoin es como si fuese el número de cliente del banco con la diferencia que nadie conoce a quien pertenece la dirección.

En Bitcoin no existe un saldo de las direcciones, sino que se conforma por la totalidad de las transacciones vigentes. La base de datos de Bitcoin contiene todas las transacciones que se hicieron en ella desde su creación.

Cuando alguien decide hacer una operación en Bitcoin lo hace creando una transacción. Suponga el lector que Pedro envía 32 BTC a María utilizando los 10 BTC que previamente había recibido de Juan, los 14 BTC que previamente había recibido de Luis y los 10 BTC que previamente había recibido de Ana (ver figura 1).

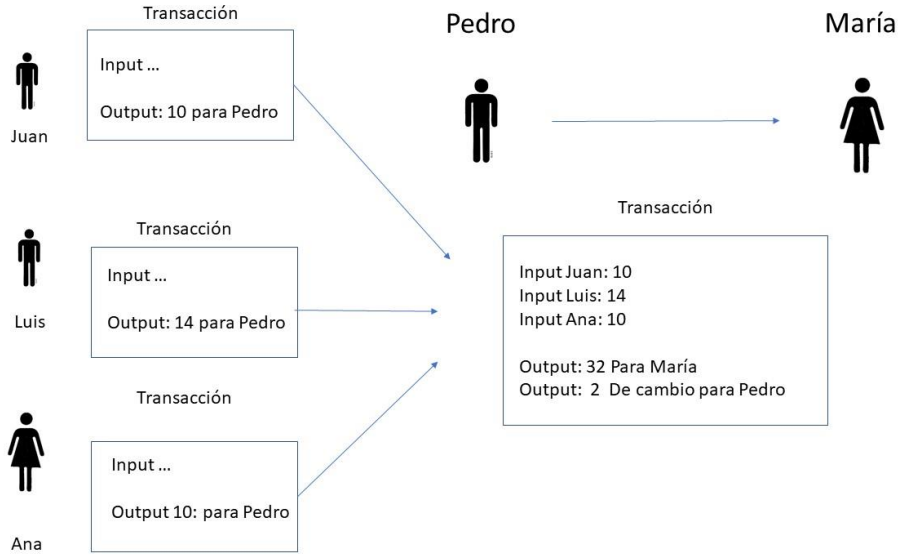
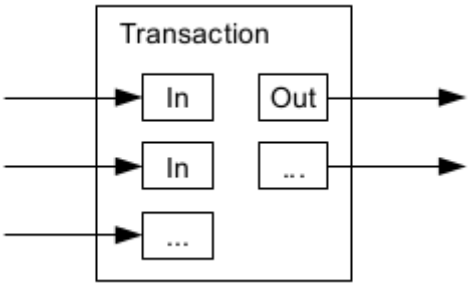


Figura 1

En este ejemplo la transacción que genera Pedro tendría tres inputs de 10, 14 y 10 BTC respectivamente (que están referenciados a la transacción que les dio origen) y dos outputs, uno con los 32 BTC asociados a la dirección de María a la cual se transfieren y un output con 2 BTC asociados a la dirección de Pedro que es la diferencia entre 10 + 14 + 10 -32 (lo que de alguna manera se podría denominar como cambio).

De lo expuesto se pude generalizar una transacción de la siguiente forma:



Una transacción contiene uno o muchos inputs (hay un tipo de transacción que no responde a esta regla pero que no hace a lo sustancial). Contiene la cantidad de inputs necesarios para poder igualar o superar la cantidad que se quiere pasar a otra dirección. Además, la transacción contiene uno o dos outputs, uno con la cantidad que transfiere y otro con la cantidad que devuelve (si es que quedara un remanente). La regla es qué si se necesita utilizar un output de una transacción anterior, debe ser utilizado en su totalidad como input de una nueva transacción. Y si hay un excedente se devuelve como otro output. En definitiva, el saldo de una dirección se conforma por los outputs no utilizados (o no consumidos) en otra transacción.

De esta forma es que se puede ver a Bitcoin como un enorme “libro contable” (por ahora se lo llamará así para ser más claro en la explicación) que almacena todas las transacciones desde que fue creado.

Este gran “libro contable” que contiene todas las transacciones está replicados (como si estuvieran espejados) en todos los nodos de la red de Bitcoin. Es decir, que todos los nodos (con una excepción que después se explicará) tiene todas las transacciones de Bitcoin desde su creación (ver figura 2)

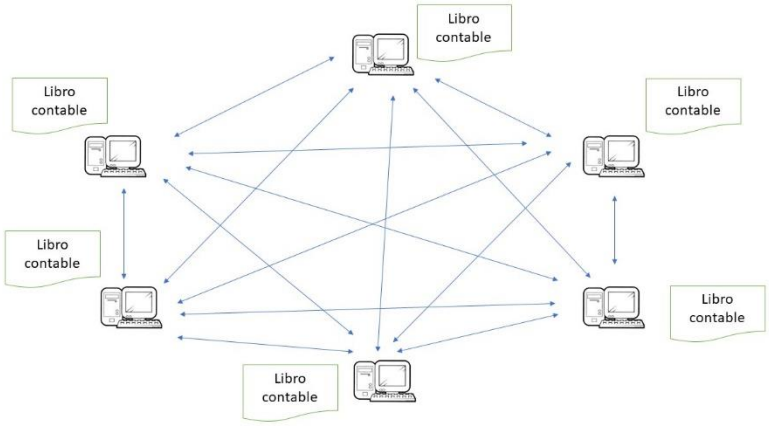


Figura 2

Cualquier persona que se quiera convertir en un nodo de Bitcoin (con la excepción ya anunciada) al instalar el software en su computadora recibirá todas las transacciones de la red de Bitcoin y al finalizar (luego de varios días de bajar información) se igualará a todos los nodos Bitcoin.

Bitcoin está asentada sobre una red P2P (peer-to-peer, red de pares, red entre iguales o red entre pares) que hace referencia a un tipo de arquitectura de aplicaciones. Es una red de computadoras en la que todas funcionan sin clientes ni servidores fijos, sino que se comportan como iguales entre sí. Es decir que cada nodo actúa simultáneamente como cliente y como servidor respecto a los demás nodos de la red. Este tipo de redes han sido

muy difundidas para el intercambio de documentos, músicas y películas. Los ejemplos más recordados de software P2P son Ares y BitTorrent.

6- ¿Cómo se logra la confiabilidad de Bitcoin?

Los bancos basan su confiabilidad, básicamente, en su nombre de marca y en el andamiaje jurídico de cada país en particular. Las personas tienen confianza en que los bancos mantienen estricto control sobre los sistemas informáticos y que su dinero, en cuentas, está en total resguardo. En consecuencia, ¿cómo puede darse confianza a la información de la base de datos de Bitcoin que se encuentra en computadoras cuyos dueños son absolutamente desconocidos y que pueden ingresar o salir de la red de Bitcoin cuando lo desean?

La confianza de Bitcoin se basa en 3 elementos:

1. La cadena de bloques o blockchain: esta herramienta tiene por objetivo que todos los nodos tengan la misma información y que la misma no sea adulterada.
2. El uso de claves asimétricas: esta tecnología permite que los BTC solo puedan ser utilizado por sus dueños, que nadie pueda conocer sus identidades y que la información no sea adulterada.
3. Software libre: Para lograr la confiabilidad del código utilizado.

6.1- Cadena de bloques

La cadena de bloques (en inglés *blockchain*) es una de las propuestas más importantes que desarrolló Bitcoin para asegurar la confiabilidad, de lo que en este artículo se ha venido denominado "libro contable". Recuerde el lector que este "libro contable" está replicado en miles de computadoras. Por lo tanto, una de las necesidades imperiosas de esta propuesta es la de garantizar:

a) Que todos estos "libros contables" sean iguales.
b) Que las transacciones estén en un orden cronológico inalterable ya que, de lo contrario, un input de una transacción podría estar haciendo referencia a un output de una transacción anterior inexistente.

Una de las mayores garantías de Bitcoin es que miles de computadoras, independientes, publiquen este "libro contable" y que en ellas la información sea igual. Las transacciones se agrupan en algo que se denomina bloque. El bloque es un contenedor de transacciones que tiene la capacidad de almacenar un promedio de 5.000 transacciones en 1 MB (varía en función de la cantidad de bits de cada transacción). Si las transacciones deben estar en orden cronológico también lo deben estar los bloques. Para mantener el orden cronológico, cada nuevo bloque se encadena al anterior y así sucesivamente. Esta cadena de bloques es lo que, en este artículo, se ha venido denominado "libro contable" (ver figura 3).

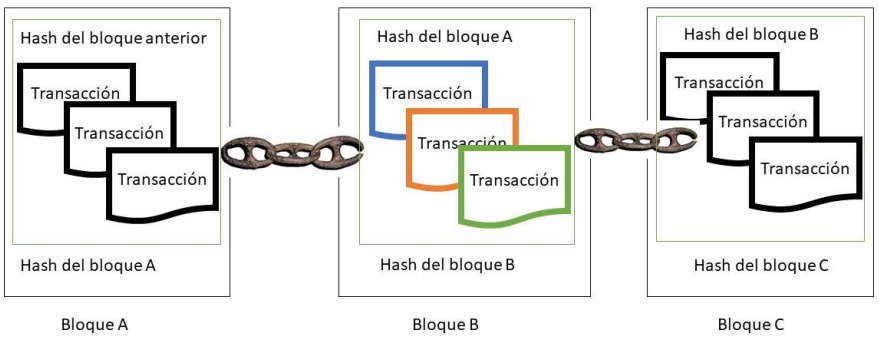


Figura 3

El encadenamiento de los bloques es lo que impide que alguien intente alterar bloques anteriores. El mecanismo de encadenamiento consiste en generar para cada bloque un hash utilizando, como entrada, los datos de todo el bloque incluido el hash del bloque anterior. Cualquier alteración a un bloque incluido en la cadena haría inconsistente a los bloques subsiguientes. Esto hace a la cadena de bloques técnicamente inalterable.

Bitcoin es una red descentralizada a lo largo y ancho de todo el mundo. Cada vez que se crea una transacción en cualquier nodo de la red, está debe propagarse al resto de los nodos (ver figura 4). Por muy veloces que sean las redes esta propagación no es instantánea, existe una demora. Esta demora generó un gran desafío para la red descentralizada. Para entender este desafío el lector debe considerar que:

1. Todos los nodos deben reciben las transacciones de toda la red para introducirlas dentro de un bloque.
2. Todos los nodos generan transacciones simultáneamente y se cruzan unas con otras

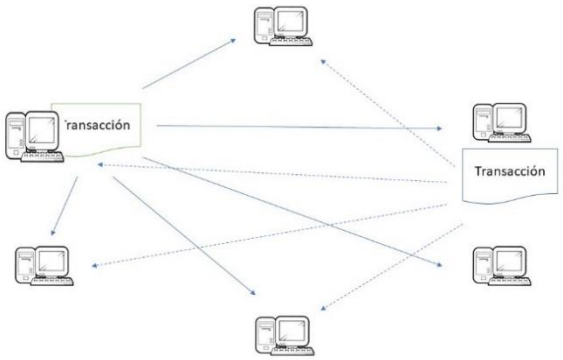


Figura 4

Por la demora antedicha, no todos los nodos introducen dentro del bloque las mismas transacciones y en el mismo orden (ver figura 5). Como ya se explicó, las transacciones hacen referencia a transacciones anteriores en un orden cronológico. Por lo tanto, si todos los nodos tuvieran ordenadas las transacciones dentro del bloque de diferente forma seria una situación de segura inconsistencia en corto tiempo. Además, esta demora podría permitir que un nodo, al hacer una transacción, esté utilizando un output que otro nodo en otra transacción ya gastó (lo que se denomina doble gasto). En consecuencia y en función de mantener un orden cronológico, es de vital importancia que la red decida quedarse con un único bloque de entre todos los que se están generado simultáneamente en todos los nodos. Para resolver cual es el bloque que definitivamente se incorporará a la cadena de bloques, se utiliza un mecanismo al que se denomina prueba de trabajo (en ingles *proof of work*).

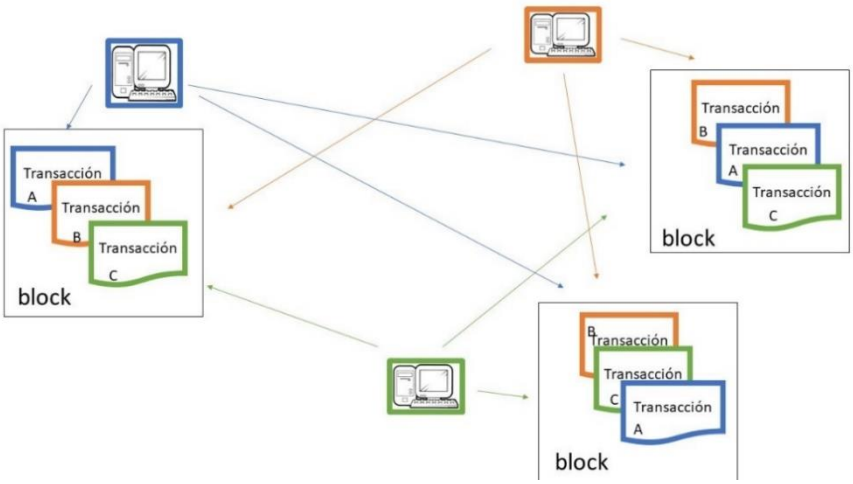


Figura 5

6.1.1- Prueba de trabajo

En Bitcoin existen distintos tipos de nodos (ver punto 6.1), la prueba de trabajo es una tarea que realiza un tipo de nodo al que se denomina “minero”. Los nodos mineros son los responsables de decidir cuál es el bloque que formará parte de la cadena de bloques (o bloque confirmado). Cuando un nodo minero completa un bloque comienza a realizar la prueba de trabajo. Este proceso se denomina minería y tiene por objetivo decidir cuál es el bloque que será incorporado a la cadena de bloques. El proceso de minería pone en competencia a todos los mineros para lograr confirmar bloques. La prueba de trabajo, que deben realizar los mineros, consiste en genera el hash que encadena el bloque con el bloque anterior. El que primero logre obtener el hash de su bloque será el minero con el boque ganador (que será el bloque confirmado).

La competencia por el lograr el hash es una tarea de gran esfuerzo computacional. Para lograr este hash el minero debe tomar como input los datos del bloque y como salida debe generar un *string* de 32 bytes (para este proceso se utiliza el hash SHA256). Pero existe una restricción especial a la generación de este proceso, que consiste en que el resultado del hash debe comenzar con una cierta cantidad de ceros como comienzo del *string* (cadena de caracteres). Esta tarea es muy exigente ya que la única manera de encontrar este hash es haciendo suposiciones aleatorias. Algo así como adivinar la combinación de una caja de seguridad. La complejidad de encontrar este hash es tan grande que una computadora normal podría estar varios años tratando de encontrarlo. Pero como todos los nodos de la red lo están intentando simultáneamente este proceso, actualmente, está durando unos 10 minutos hasta que uno de ellos de con el hash deseado. El primer nodo que resuelve el problema difundirá su bloque al resto de la red. El resto de los nodos verifican su validez o de lo contrario será rechazado. Los nodos al recibir el bloque deberán verificar que:

a) Los BTC hayan sido utilizados por sus legítimos poseedores.
b) Que los inputs no hayan sido anteriormente consumidos.
c) Que el hash obtenido en la prueba de fuerza sea correcto.

Es muy poco probable que dos o más nodos resuelvan simultáneamente el bloque, pero puede ocurrir (ver figura 6).

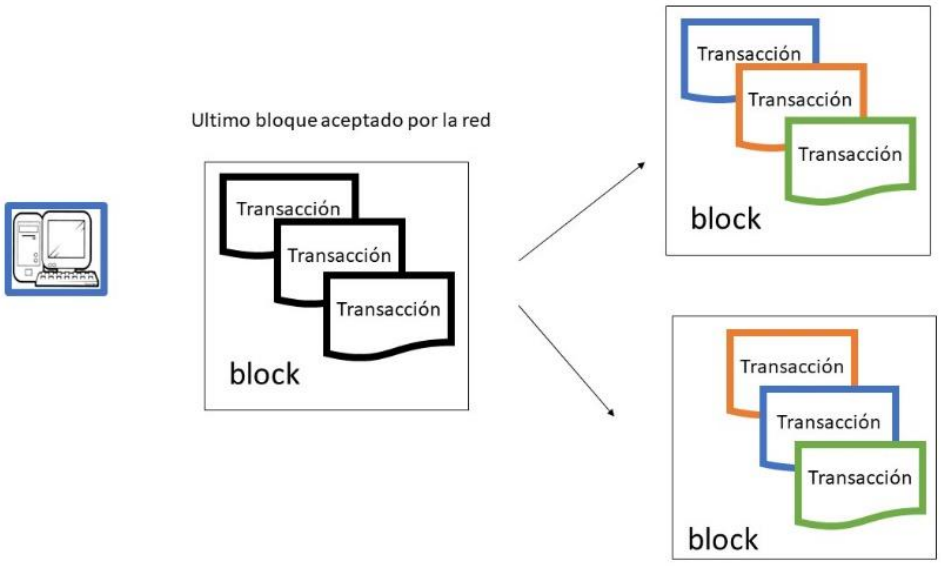


Figura 6

La forma de solucionar este problema es que cuando aparezca un nuevo bloque resuelto (o ganador) este invalidará los bloques no encadenados a él (ver figura 7). Serían aún menos probable que esta anomalía ocurra

consecutivamente más de una vez, pero si esto sucediera se resolvería de la misma manera. Es decir que prevalece la cadena más larga.

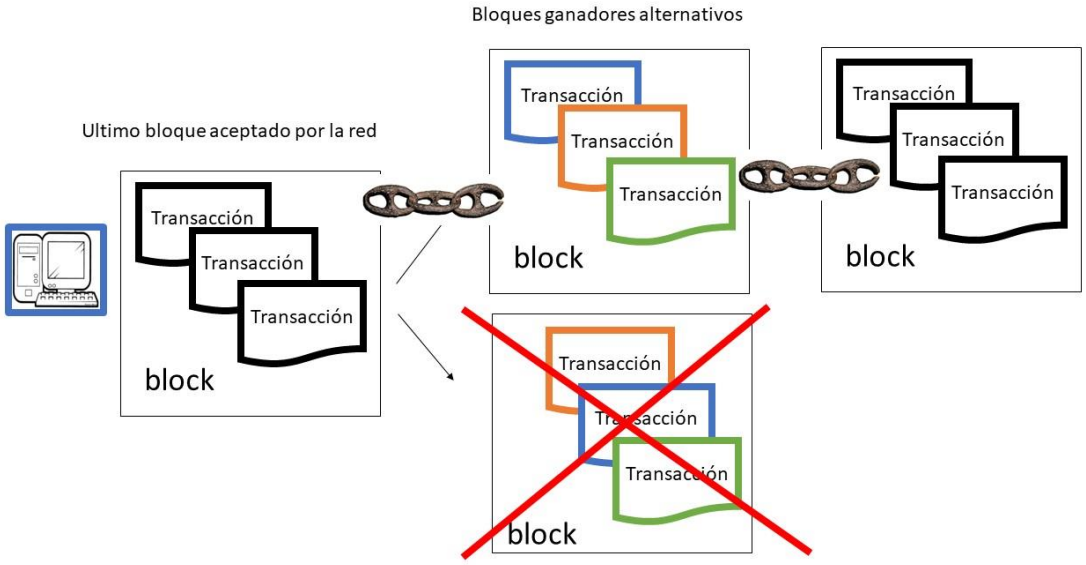


Figura 7

Las transacciones que hayan sido descartadas por no estar en los nodos definitivamente incorporados a la cadena de bloques deberán incorporarse a un bloque en formación.

La posibilidad de la existencia, al final de la cadena, de bloques aún no confirmados genera una cierta inestabilidad. Suponga el lector que alguien intentara lograr un doble gasto para estafar a alguien (es decir usar un output de una transacción anterior en inputs de diferentes transacciones posteriores). Para ello debería lograr generar dos bloques alternativos, por ejemplo: los bloques: A y B (ver figura 8). El bloque A debería tener un gasto X y el B debería tener un gasto Y. Luego, quien este intentando el fraude, debe lograr un nuevo bloque ganador C encadenado al bloque A para que se descarte el bloque B con un doble gasto Y (este bloque sería aceptado porque el bloque B fue descartado). Cuando el gasto Y del bloque descartado vuelva a tratar de incorporarse a un bloque en formación no será aceptado.

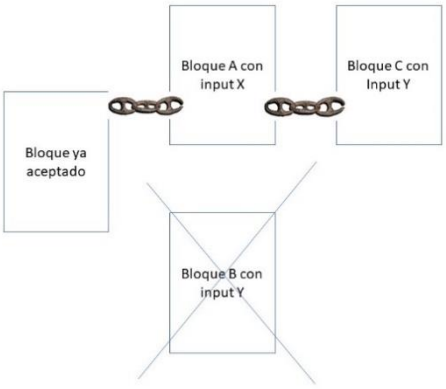


Figura 8

Para que alguien logre este fraude debería tener una capacidad de cómputo, terriblemente, poderosa. Si tuviera una capacidad de cómputo mayor al 50 % de toda la red de Bitcoin solo tendría el 50 % de probabilidades de lograrlo y tan solo por un muy corto plazo. Por este motivo, y siendo extremadamente precavido, se recomienda que el usuario de Bitcoin no de una transacción por válida hasta que el bloque, en el que fue incorporada su transacción, no tenga añadidos a la cadena 6 bloques posteriores.

Los motivos que tienen los mineros para realizar este trabajo es que el ganador en el proceso de minar obtiene una recompensa. Por cada bloque minado con éxito, un minero, obtiene una recompensa de BTC 12,5. Es decir, que cada vez que un nodo minero se pone a trabajar tiene una probabilidad, relacionada a su capacidad de cómputo y su suerte, de ganar BTC 12,5. Esta recompensa, además de ser un estímulo a los mineros, es la forma de agregar BTC al mercado. Como el crecimiento de Bitcoin ya fue planificado antes de su lanzamiento, en poco tiempo más los mineros pasarán a obtener 6,25 por bloque minado con éxito. El objetivo de esta medida es incorporar BTC en una cantidad relacionada con el crecimiento de la red. Se calcula que existen más de 1.600.000 computadoras minando distintas criptomonedas. Cuando un minero logra ser el ganador y obtener su recompensa, esta se implementa mediante una transacción. Es una transacción especial porque solo tiene un output asociado a la dirección del minero por los BTC 12,5 (no tiene inputs). Esta no es la única motivación de los mineros para realizar su trabajo. Además, existe la comisión que el minero puede decidir cobrar. Esto requiere una explicación más completa que se dará al final de documento en el punto 8. Es de destacar sobre los mineros, que la mayoría de ellos tiene sus computadoras instaladas en China ya que en este país el costo de la energía es muy bajo. Los mineros invierten grandes sumas de dinero para aumentar sus capacidades computacionales ya que cuanto más poder tengan más posibilidades tienen de obtener bloques ganadores.

6.1.2- Distintos tipos de nodos

En Bitcoin existen tres tipos de nodos:

a) Nodos ligeros: estos nodos solo emiten transacciones, trabajan a modo broadcast.

b) Nodos completos: esto nodos emiten transacciones y verifican la validez de las transacciones. Son nodos que necesitan utilizar el total de la cadena de bloques.

c) Nodos mineros: estos nodos emiten transacciones, las verifican y realizan el trabajo de minería. También, requieren de la totalidad de la *blockchain*.

6.2- Direcciones

Para entender esta explicación recomiendo que el lector esté familiarizado con la mecánica de la criptografía de claves asimétricas y el significado de los términos: clave pública y clave privada.

Como ya se dijo, la dirección de Bitcoin es un conjunto de bit a los cuales se asocian los Inputs y los Outputs. Las direcciones de Bitcoin tienen la especial particularidad de que son claves púbicas (C.Pu). En Bitcoin solo se sabe que cantidad de BTC tiene una determinada dirección o C.Pu. Se desconoce el poseedor de la clave privada (C.Pr.) asociada a la C.Pu correspondiente (o dirección), por este motivo, es que en Bitcoin se desconoce a las personas que poseen BTC.

Para que se entienda mejor se volverá por un momento al ejemplo de Pedro de la figura 1. Imagínese que Pedro desea realizar una transacción en Bitcoin. Para este fin, Pedro necesitara una C.Pu sin la cual no podrá hacer nada en Bitcoin. Para obtenerla, Pedro debe elegir un numero de 256 bits (puede ser generado automáticamente). Este número es el que Pedro utilizará como su Clave Privada (C.Pr.) para, desde ella, generar su C.Pu y para firmar digitalmente las transacciones. Las direcciones se crean con un programa que se denomina monedero que se explicará en el punto 7. El programa monedero toma como entrada del proceso al número elegido de 256 bits y le

aplica varios algoritmos matemáticos (SHA-256 y RIPEMD160) después de los cuales queda generada la C.Pu. Pedro utilizará su C.Pu para recibir BTC y, para desde ella, enviar BTC.

En Bitcoin las transacciones transfieren BTC desde una dirección a otra dirección. Cuando una persona transfiere BTC a una determinada dirección debe indicar la forma en que el receptor deberá demostrar su derecho a utilizarlos. Recuerde el lector que cuando se crea una transacción se deben indicar los inputs (desde donde se obtienen las BTC) y los outputs (el destino de las BTC). En los outputs se crea un script (que es un pequeño programa) donde se estipula como deberá demostrar, el poseedor de la dirección de destino, ser su verdadero titular (esta demostración se deberá efectuar cuando se pretendan gastar los BTC). Por lo tanto, un output está formado, básicamente, por: la dirección de destino, un script y la cantidad de BTC. Normalmente, el script exige al titular de la C.Pu de destino demostrar con una firma digital, ser el verdadero titular de la dirección. En el punto 6.2.2 (direcciones multifirma) se explicará que algunas transacciones pueden requerir mas de una firma digital.

6.2.1- Firma digital

Cuando alguien crea una transacción, como ya se dijo anteriormente, debe demostrar con una firma digital (o más) ser el verdadero poseedor de los BTC. El algoritmo de firma digital utilizado en Bitcoin no es el conocido RSA, que utiliza la mayoría de los países para firmar digitalmente documentos digitales (como es el caso de Argentina), sino que utiliza ECDSA (Elliptic Curve Digital Signature Algorithme). Como es un algoritmo que requiere un conocimiento de matemática avanzada no se explicará la matemática de la firma digital sino solo su funcionalidad.

Para explicar cómo se firma digitalmente una transacción se volverá al ejemplo de Pedro (ver figura 9). Recordando el ejemplo: Pedro envía 32 BTC a María utilizando 10 BTC recibidos de Juan, 14 BTC recibidos de Luis y 10 BTC recibido de Ana. El programa de monedero, que utiliza Pedro, debe verificar cuales son las exigencias de los scripts que crearon Juan, Luis y Ana en los outputs de las respectivas transacciones que ellos generaron originalmente. Suponiendo que los tres (Juan, Luis y Ana) solo exigieron a Pedro una firma (la de Pedro) el programa monedero que crea la transacción de Pedro deberá hacer lo siguiente (ver figura 10): Tomar como inputs todos los datos de la transacción, a los mismos aplicarle la C.Pr. de Pedro y generar un conjunto de dígitos (a lo que se denomina firma digital) y guardarlos en la misma transacción.

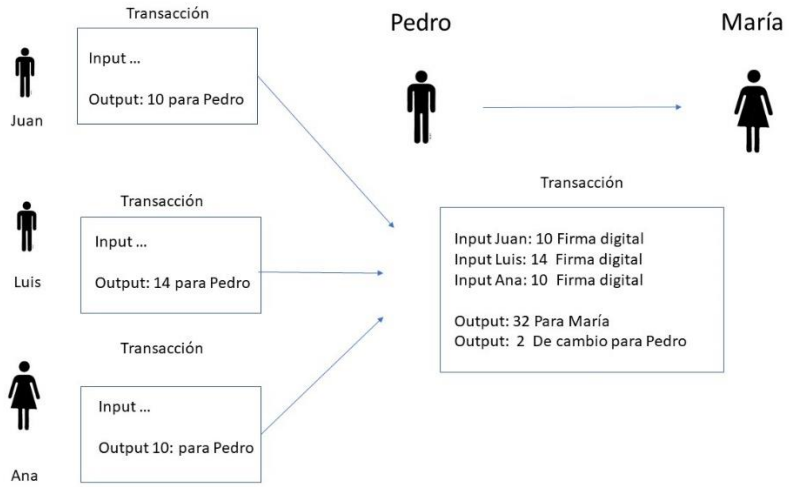


Figura 9

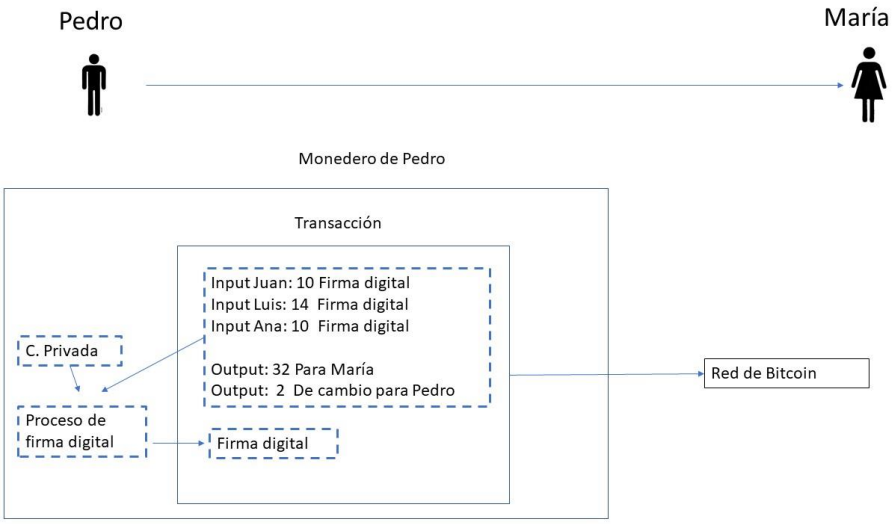


Figura 10

Los mineros de Bitcoin deben controlar la firma antes de admitir la transacción en un bloque. Para lo cual realizan un proceso (ECDSA) que toma los datos de la transacción, la dirección (C.Pu de Pedro) y la firma digital. Si el proceso da un resultado exitoso la transacción se acepta, de lo contrario la transacción se rechaza.

Este proceso de firma digital garantiza que los BTC solo puedan ser gastados, únicamente, por sus correspondientes titulares sin exponer en ningún momento sus identidades personales.

6.2.2- Direcciones multifirma

Las direcciones multifirma son direcciones Bitcoin que, a diferencia de las direcciones Bitcoin estándar, pueden estar gestionadas por muchas personas al mismo tiempo. En las direcciones multifirma, la firma para autorizar la transacción se crea de forma colectiva. Ahora bien, uno de los detalles más importantes es que, en este tipo de direcciones, es posible configurar el número mínimo de firmas que se necesitarán para autorizar los outpus. Es decir, se puede crear una dirección multifirma a partir de tres C.Pr, pero que necesite solo de dos de ellas (sin importar cuales) para poder utilizarse. Es lo que se conoce como una “dirección Bitcoin multifirma 2 de 3”. Y de la misma forma pueden ser 3 de 5, 4 de 7, 6 de 10, incluso 2 de 2, etc. En resumidas cuentas, para crear una dirección multifirma se necesita indicar cuántos serán los participantes y cuál es el mínimo de participantes que serán necesarios para autorizar el gasto.

6.3-La confiabilidad del software

Para asegurar el buen funcionamiento de las reglas de Bitcoin es, fundamental, que los actores principales de la red, los mineros, utilicen software autorizado por Bitcoin. Bitcoin se desarrolló bajo el esquema de código abierto lo que significa que el código fuente puede ser examinado por todo el mundo. Pero una de las principales debilidades de Bitcoin es que no existe un modelo de homologación (aprobación) de software democrático. Originalmente, Satoshi Nakamoto, quien fue el principal desarrollador del software de Bitcoin, mantuvo el control de todo el software que se liberaba para la red, al irse, éste le entregó esta responsabilidad a Gavin Andersen quien en abril de 2014 se la cedió a Wladimir J. van derLaan.

Existen muchos programadores que colaboran en el desarrollo deBitcoin pero la decisión de poner un programa a funcionar en la red es solo de Wladimir. Hay otros tres colaboradores con mucha influencia en la red de Bitcoin que son: Jeff Garzik, Gregory Maxwell y Pieter Wuille. El programa fundamental de Bitcoin se denomina Bitcoin Core. La última versión de Bitcoin Core es la 0.16.0 que se puede obtener en https://bitcoincore.org/bin/bitcoin-core-0.16.0/

El código para el proyecto Bitcoin se desarrolla en un solo lugar o repositorio utilizando un Github (es un software para gestionar proyectos de desarrollo de software y control de versiones). La versión oficial del repositorio Bitcoin es conocido como el repositorio principal. Los desarrolladores pueden crear sus propias versiones del repositorio. Esto les permite trabajar en sus propios cambios del código. Pueden modificar sus versiones tanto como quieran. En cualquier momento del trabajo, pueden solicitar que su versión sea incluida en un repositorio denominado principal como una "extracción". Una vez que esté en el repositorio principal, los otros miembros que participan en el proyecto pueden revisar y comentar sobre dicha "extracción". Si a suficientes personas les parece apropiado el cambio sugerido en la "extracción", éste puede llegar a ser incluido en el Bitcoin Core pero solamente si Van derLaan lo aprueba. Las discusiones menos formales sobre el desarrollo se realizan en el canal #bitcoin-dev de irc.freenode.net.

En agosto de 2017 esta forma, poco democrática, de la gestión del cambio de Bitcoin creó seria desavenencias ente los principales desarrolladores de Bitcoin. Como consecuencias de ellas se generó una ruptura que dio lugar al surgimiento de Bitcoin Cash. Hoy existe Bitcoin y Bitcoin Cash y son dos criptomonedas independientes.

En 2017 el MIT Media Lab del Massachusetts Institute of Technology (MIT) dió un importante respaldo a Bitcoin anunciado la creación del Bitcoin Development Fund. Esta institución cubre los sueldos de los desarrolladores principales del Bitcoin Core. El objetivo es ir creando un "ambiente académico neutral", y apoyar eventos que promuevan el desarrollo del protocolo Bitcoin. Hoy el software de Bitcoin se produce bajo licencia MIT.

7- Monederos de Bitcoin

Los monederos o wallets de Bitcoin (también se utilizan los nombres de "cartera" y "billetera") almacenan las C.Pr. que se necesitan para crear transacciones de bitcoins. A diferencia de las transacciones que son de público acceso y están distribuidas en toda la red de Bitcoin, las claves privadas, deben cuidarse celosamente. Cualquiera que accediera al conocimiento de una C.Pr podría apoderarse de las BTC que su titular poseyera. Si algún usuario pierde la C.Pr perderá sus BTC porque no hay forma de poder generarla a partir de la dirección (C.Pu). En síntesis, los monederos son los programas que permiten crear transacciones en la red y proteger las claves privadas.

Existen cuatro tipos principales de monederos o wallets:

a) Monederos para PC
b) Monederos para teléfonos móviles o tabletas
c) Monederos on line en internet
d) Dispositivos físicos diseñados para ser monederos Bitcoin

7.1- Monederos para PC

La característica principal de este tipo de monederos es que almacenan la C.Pr. en la computadora propia. La clave privada suele estar encriptada para otorgar un grado de seguridad extra en caso de que la seguridad de la PC se vea comprometida.

Los más utilizados son:

a) Bitcoin Core o Bitcoin-qt: Este monedero requiere descargar la cadena de bloques por completo y, además, actúa de nodo para que la red verifique la cadena de bloques.

b) Electrum: Es una cartera muy popular porque no requiere descargar la cadena de bloques completa y, por tanto, es mucho más rápido y algo menos seguro que la cartera Bitcoin-qt. Otra de las ventajas que ofrece, es la creación de lo que se conoce como semilla y que permite poder crear una copia del monedero sin ninguna información adicional. La semilla, que es una secuencia de números y/o palabras que se pueden guardar en un papel, permite restaurar el monedero en otro ordenador en caso de que se borre.

7.2- Monedero para teléfonos móviles y tablets

Este tipo de monederos son los más empleados para realizar pequeños pagos, suelen descargar una pequeña parte de la cadena de bloques confiando en que otros nodos tengan la información correcta de la cadena de bloques.

Los monederos o carteras Bicoin para móvil más conocidas son las siguientes: Bitcoin wallet, Blockchain.info y Kipochi.

7.3- Monederos on line en Internet

Son los más empleados, más fáciles de usar y los menos seguros. Este tipo de monedero almacena la clave privada de los usuarios en un servidor controlado por una empresa. Es decir, el cliente no conoce ni tiene la clave privada del monedero y, por tanto, la responsable de mantener y guardar esa clave privada es la empresa que ofrece el servicio de monedero.

La gran ventaja de los monederos on line es la facilidad de uso y la accesibilidad, pues son accesibles desde cualquier lugar y permiten realizar pagos y transferencias con rapidez. Son ideales para tener una pequeña cantidad de BTC y poder operar con rapidez y comodidad.

Este tipo de monederos son ofrecidos por casi todas las casas de cambio, pues cuando se realiza la compra de Bitcoins se depositan de forma automática en un monedero on line.

Algunos de los monederos on line más empleados son los siguientes: Blockchain.info, Coinbase, Kraken y OKCoin.

7.4- Dispositivos físicos

Existe lo que se llama monedero en papel, estos son programas que permiten generar en forma offline una C.Pr y su correspondiente C.Pb. Estas pueden almacenarse en un soporte físico o imprimirse en un papel. Estos monederos han sido pensando, solo, para recibir BTC en forma absolutamente segura. Con, simplemente, informar la dirección podrán recibir BTC en esa dirección. La dificultad es que para utilizar los BTC recibidos deberá recurrir a algún otro tipo de monedero. La forma segura de trabajar con los monederos en papel es gastar por completo los BTC de la dirección (con alguno de los otros monederos) y luego desecharla. Para volver a recibir BTC se deberá generar un nuevo juego de claves. Estos monederos pueden imprimir la secuencia de dígitos de las claves o generar un código QR para facilitar su importación a otros monederos al momento de querer gastar los BTC recibidos.

También existen los monederos hardware. El más comercializado es Trezor. Se conectan a la PC o al celular por un puerto USB. Requieren de un programa instalado en la PC o el celular que interactúa con el dispositivo monedero.

Los pasos para usar este tipo de monedero son los siguientes:

a) Con el programa del PC o del celular se genera la transacción (estando on line).
b) Se conecta el monedero.
c) El programa de la PC (en offline) envía la transacción al programa hardware del monedero.
d) El programa hardware del monedero firma la transacción y se la devuelve al programa de la PC (en off line).
e) Se desconecta el monedero.
f) El programa de la PC (en on line) envía la transacción a la red.

8- Comisiones

Otra de las motivaciones que tienen los mineros para realizar su trabajo es la de obtener una comisión. Cuando se genera una transacción, puede ser que la suma de los inputs sea mayor que la de los outputs. Esta diferencia es la

que se deja como comisión para los mineros que es a voluntad de quien genera la transacción. Pero se debe tener en cuenta que si no se da una comisión puede ocurrir que la transacción demore días en ser aceptada o no sea aceptada nunca (ningún minero decide incorporarla a ningún bloque). Si la comisión es alta la transacción será aceptada rápidamente, cuanto más baja sea la comisión más tardará en ser aceptada. Por lo tanto, la comisión está estrictamente relacionada a un libre juego de oferta y demanda.

Los monederos on line, fundamentalmente, obtienen sus ganancias en la comisión que cobran al cambiar dinero de curso legal por BTC o viceversa.