Bitcoin

Oliver Thiessen

Universidad Católica Nuestra Señora de la Asunción olithiessen@gmail.com
http://www.uca.edu.py

Abstract. Este paper es un informe del estado del de Bitcoin, la primera moneda digital criptográfica. Se explica en que consiste, como surgió, el funcionamiento con un cierto nivel de detalles técnicos y el estado de la economía.

Key words: Bitcoin, Satoshi Nakamoto, moneda criptográfica, moneda digital, economía, peer-to-peer.

1 Introducción

El comercio en internet se ha tornado un comercio que confía exclusivamente en instituciones financieras que sirven como terceros de confianza. Este sistema funciona bastante bien para la mayoría de los casos, pero sufre de algunas debilidades: No son posibles las transacciones completamente irreversibles, ya que las instituciones financieras no pueden evitar mediar las disputas, lo cual genera un costo, el cual sube el costo de la transacción. Esto a la vez limita el tamaño mínimo de una transacción práctica de realizarse, imposibilitando así a la posibilidad de realizarse transacciones pequeñas, y hay un costo mayor en la pérdida de la habilidad de hacer pagos no-reversibles a servicios no-reversibles. Esto aumenta la necesidad de confianza. Vendedores necesitan más información acerca de sus clientes de lo que sería necesario. Un cierto nivel de fraude se acepta como inevitable. Estos costos e incertidumbres de pago pueden ser evitadas utilizando una moneda física, pero no existe un mecanismo que permita hacer un pago por un canal de comunicación sin un tercero de confianza.

Lo que se necesita es un sistema de pagos basados en pruebas criptográficas en lugar de confianza, permitiendo a cualquier par de personas intercambiar dinero sin necesitarse un tercero de confianza.

Bitcoin es una de las primeras implementaciones de un concepto llamado crypto-currency (en inglés: cripto-moneda o moneda criptográfica). Se basa en la noción que el dinero es cualquier objeto, o cualquier tipo de registro que se acepta como pago en cambio de bienes y servicios. Bitcoin fue diseñado considerando el uso de criptografía para controlar la creación y transferencia de dinero, en vez de confiar en autoridades centrales.

Satoshi Nakamoto, creador de Bitcoin, quería que las personas sean capaces de intercambiar dinero electronicamente de forma segura sin la necesidad de una tercera parte, como lo es un banco o una compañía como PayPal. Las técnicas criptográficas en las que se basa Bitcoin permiten al usuario estar seguro que el dinero recibido es auténtico, incluso si no se confía en el pagante.

2 Historia

En el 2008, un programador conocido como Satoshi Nakamoto (el cual se cree es un alias) posteó un paper a una lista lista de correo electrónico de criptografía. Luego, en el 2009 el autor publica un software que puede ser utilizado para intercambiar bitcoins utilizando el esquema. Este software es mantenido por una comunidad open-source coordinada por 4 desarrolladores principales. Según Jeff Garzik, desarrolador de Bitcoin y fundador de Bitcoin Watch (un organismo que monitorea la economía Bitcoin), "Satoshi es una figura algo misteriosa. Yo y los otros desarrolladores ocasionalmente nos comunicamos con él vía e-mail, pero no siempre el responde. Esto y el foro son las unicas formas en que cualquier persona se ha comunicado con él." En su perfil de P2P Foundation, Nakamoto dijo ser originario de Japón. Se considera que el programador (o tal vez el grupo de programadores) eligió ocultar su identidad debido al miedo que le tienen a los gobiernos.

Bitcoin fue lanzado para el uso en 2009. Los usuarios utilizan software libre distribuido en una red peer-to-peer (P2P). Esto creó una agitación entre los activistas que plantean a la criptografía como un servicio de empoderamiento de las libertades civiles. Bitcoin fue adoptado como un sistema de donaciones resistente a cesuras por organizaciones como Electronic Frontier Foundation, Freenet y Wikileaks.

3 Funcionamiento

Bitcoin utiliza la criptografía asimétrica. Todas las transacciones son públicas y almacenadas en una base de datos distribuida. La red implementa un servidor de tiempo (timestamp server) distribuido para evitar el doble gasto, utilizando la idea de cadenas de pruebas de trabajo (proof-of-work).

El algoritmo publicado por Nakamoto está implementado en C++.

3.1 Direcciones

Bitcoin se basa en la criptografía de clave pública. Cualquier persona en la red Bitcoin tiene una billetera conteniendo un número arbitrario de pares de claves.

Las claves públicas del usuario son transformadas en direcciones Bitcoin (que actúan como destinos de pagos). La longitud de la dirección es de 160 bits. Las claves privadas correspondientes se utilizan para autorizar pagos realizados con la billetera del usuario. Las direcciones en sí no contienen información sobre el usuario. La forma humana de leer las direcciones se representa mediante cadenas de números y letras de alrededor de 33 caracteres de longitud, siempre empezando con el número 1.

Ejemplo: 1L6givWWH5rYU8AzaRk6AA9s5fCRtwmQ7L

3.2 Minería de coins

Para que tengan algún valor, la creación de los coins tiene que ser limitada. Un usuario que esta generando coins, está ejecutando un programa que busca constantemente la solución a un problema matemático complicado. Este programa se llama "bitcoin miner" (minería de bitcoins). La dificultad se ajusta automáticamente de forma regular de modo que el número de soluciones encontradas globalmente, por cualquier usuario, es constante con un promedio de 6 por hora. Al encontrarse una solución, el usuario puede informarle a todos de la existencia de la misma, junto con otra información, empaquetados en un bloque.

Cada 4 (cuatro) años, la cantindad de bitcoins que puede ser generada en un bloque se reduce un 50%. Los bloques que fueron creados por un usuario maligno que no sigue las reglas serán rechazados por cualquier otro usuario. El resultado de esto es que nunca existirán más de 21 millones de bitcoins.

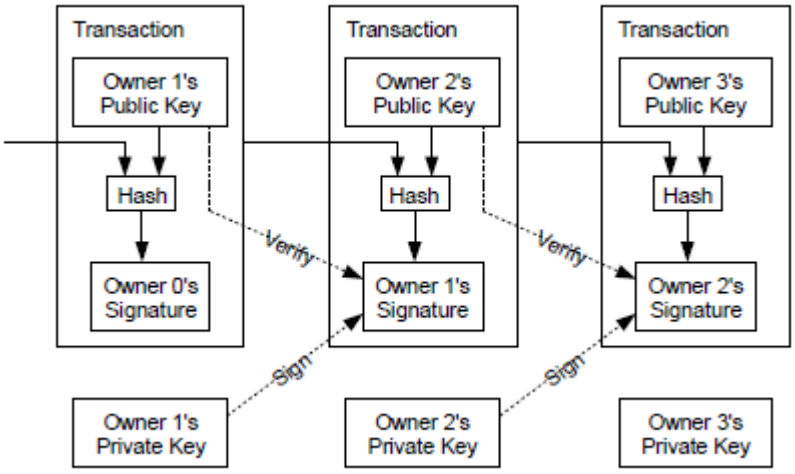
Como la cantidad de bitcoins que incentiva a la generación de bloques disminuirá, los usuarios algún día pagarán por los costos de hardware y electricidad cobrando honorarios por las transacciones. El emisor del dinero puede voluntariamente pagar un honorario a quien encuentra el bloque siguiente. Esto incentivará al usuario a incluir la transacción en un bloque de forma más rápida.

3.3 Transacciones

Cada bitcoin contiene la dirección de la billetera del dueño actual. Cada usuario puede crear cuantas billeteras quiera. Cuando un bitcoin perteneciente al usuario A se transfiere al usuario B, A renuncia a la posiesión del bitcoin poniendo como dirección a la dirección de la billetera de B y firmando el resultado con la clave secreta de A. Debido al método criptográfico asimétrico, nadie puede confirmar esta firma y la clave privada no puede ser determinada a partir del bitcoin. El resultado es enviado mediante broadcast en un mensaje, la transacción, en la red peer-to-peer. El resto de los nodos de la red validan la firma criptográfica y los montos de la transacción antes de aceptarlo.

Se puede definir una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere al coin al proximo firmando digitalmente el hash de la transacción previa y la clave pública del proximo dueño y añadiendo los dos al fi-

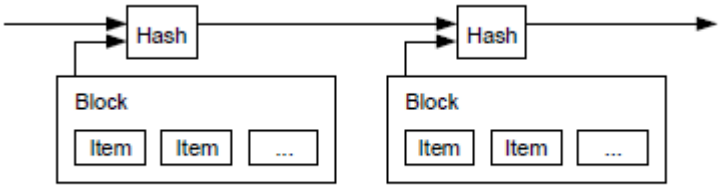
nal del coin. El receptor del coin puede verificar las firmas para verificar la cadena



de posesión.

3.4 Servidor de timestamp

El timestamp server toma el hash de un bloque de items a ponerle el timestamp y publicando el hash. Esto implica que el timestamp tuvo que haber existido al momento para poder ser parte del hash. Cada timestamp incluye al timestamp anterior en su hash, formando una cadena, con cada timestamp adicional reforzando a los anteriores.

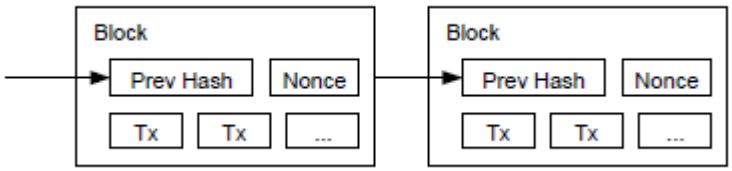


3.5 Proof-of-Work

Por definición, un sistema pruebas de trabajo (proof-of-work system en inglés, Sistema "POW") dificulta los ataques de denegación y servicio, requiriendo algún trabajo (cómputo) por parte del cliente del servicio. Este trabajo tiene la característica de la asimtería: debe ser moderadamente dificil de realizarse por el lado del cliente, pero fácil de verificarse por el lado del servidor.

El proof-of-work requiere que se busque un valor que, cuando hasheado (por ejemplo con SHA-256), resulte en un hash que empieze con una cantidad de bits 0 (zero). El trabajo requerido es exponencial a la cantidad de bits 0 requerida y puede ser verificado por un solo hash. El POW se implementa incrementando

un "nonce" (un numero arbitrario utilizado una única vez para firmar una comunicación criptográfica) en el bloque hasta que un valor que le da al bloque la cantidad deseada de bits 0 es encontrado. Una vez que la CPU hizo el esfuerzo para satisfacer al POW, el bloque no puede ser cambiado sin rehacer el trabajo. Como despues se agregan bloques a la cadena, el trabajo para cambiar el bloque significaría cambiar todos los bloques siguientes.



El POW tambien resuelve el problema de determinar la representación de la mayoría en una descisión. Si el sistema fuera basado en "un voto por IP", podría ser subvertido por cualquier persona capaz de asignar múltiples IPs. POW consta de "un voto por CPU". La mayoría en la decisión es representada por la cadena más larga, que tiene invertida la mayor cantidad de esfuerzo POW. Si la mayoría de las CPUs es controlada por nodos honestos, la cadena honesta crecerá rápidamente, sin posibilidades de que cadenas competentes le alcancen. Para modificar un bloque pasado, un atacante tendría que rehacer el POW del bloque y todos los bloques siguientes, y luego tratar de superar el trabajo de los nodos honestos. La probabilidad de que un atacante más lento alcance a los nodos honestos disminuye exponencialmente mientras se agreguen bloques.

Para compensar aumento de velocidad del hardware y el interes variante de calcular nodos en el tiempo, la dificultad del POW se determina por un promedio de bloques por hora. Si los bloques se generan muy rápido, la dificultad crece.

3.6 La red

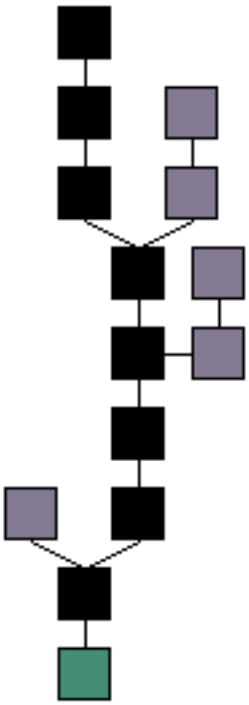
Los pasos para ejecutar la red son los siguientes:

1. Nuevas transacciones se envían por broadcast a todos los nodos
2. Cada nodo junta nuevas transacciones en un bloque
3. Cada nodo trabaja encontrando un POW para su bloque
4. Cuando un nodo encuentra un POW, lo envía por broadcast a todos los nodos
5. Los nodos solo aceptan el bloque si todas las transacciones son válidas y todavía no se gastaron
6. Los nodos aceptan al bloque mediante la creación del proximo bloque de la cadena, utilizando el hash del bloque aceptado como hash anterior.

Los nodos siempre consideran que la cadena más larga es la correcta y tratará de expandirla. Si dos nodos envían diferentes versiones del proximo bloque simultaneamente, algunos nodos pueden recibir al uno o al otro primero. En tal caso, trabajarán con el primer bloque que recibieron, pero guardarán la otra rama para el caso que se convierta en el más largo. El desempato ocurre cuando

el proximo POW es encontrado y una rama se vuelve más larga. Los nodos que estaban trabajando en la otra rama cambiarán por la rama más larga. Nuevas transacciones no necesitan alcanzar todos los nodos. Mientras alcancen muchos nodos, no tardarán mucho a entrar a un bloque. Broadcasts de bloques también toleran la pérdida de mensajes. Si un nodo no recibe a un bloque, lo pedirá cuando reciba el bloque siguiente y se da cuenta que falta uno.

Fig. 1. negro: cadena principal más larga; verde: bloque inicial; gris: bloques huérfanos.



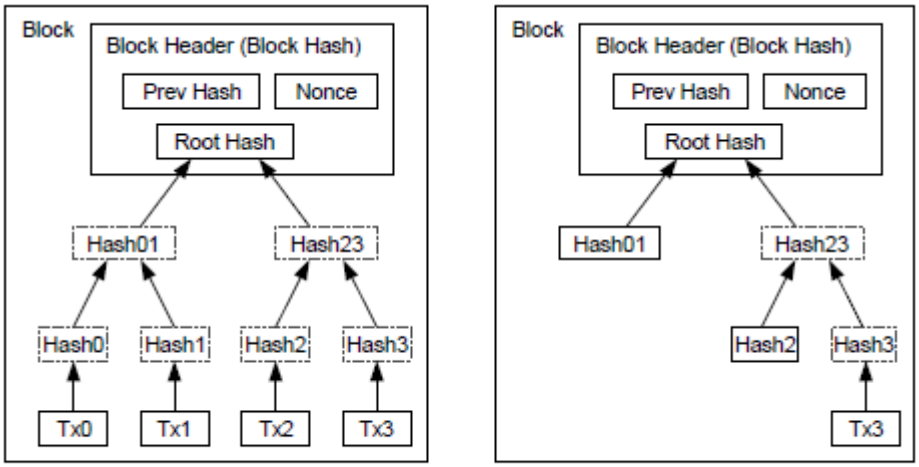
3.7 Incentivo

Por convención, la primera transacción en un bloque es una transacción especial que empieza un coin que posee el creador del bloque. Esto estimula a los nodos a apoyar a la red, y provee un método de distribuir inicialmente a los coins en circulación, ya que no existe autoridad central que lo haga. Otro incentivo son los honorarios de transacciones. Si el valor de salida de una transacción es menor que el valor de entrada, la diferencia es un honorario de transacción que retiene el nodo como incentivo. Una vez que haya suficientes coins en circulación, el único incentivo necesario serán los honorarios de transacciones, eliminando la inflación. El incentivo puede alentar a los nodos para que actúen de forma honesta. Si un

atacante codicioso es capaz de juntar más capacidad de CPU que todos los nodos honestos, tendría que decidir entre utilizarlo para defraudar usuarios robando lo que les pagó o usarlo para generar nuevos coins. El atacante debería darse cuenta que generaría más ganancias obedeciendo las reglas, que le favorecen con más coins que todo el resto en vez de desvalorizar al sistema y a sus propios bienes.

3.8 Espacio en disco

Una vez que la última transacción en un coin está en suficientes bloques, las transacciones anteriores gastadas pueden ser eliminadas para ahorrar espacio en disco. Para facilitarlo, los bloques son hasheados en un arbol de Merkele, donde solo la raíz está incluida en el hash del bloque. Bloques viejos pueden ser compactados acortando las ramas del arbol. Los hash interiores no necesitan ser almacenados.

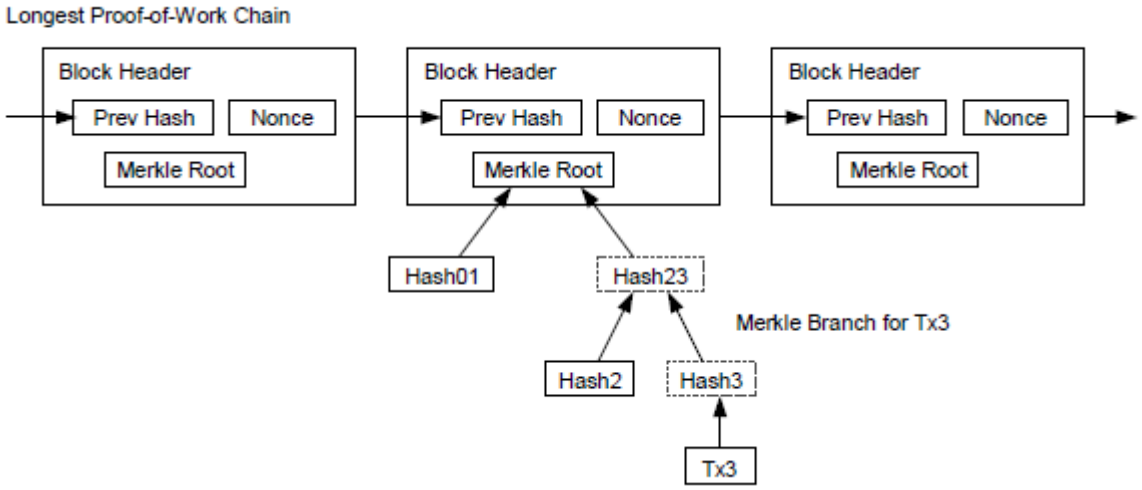


La cabecera de un bloque sin transacciones tiene un tamaño de 80 bytes. Si asumimos que se generan bloques cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por año. Con la capacidad de memoria que tienen las computadoras actualmente y la ley de Moore prediciendo el crecimiento de 1.2GB por año, se asume que el almacenamiento no deberá ser problema.

3.9 Verificación simple de pago

Es posible verificar pagos sin ejecutar un nodo completo de la red. Un usuario solo necesita una copia de las cabeceras de bloques de la cadena POW más larga, la cual puede obtener consultando nodos de la red hasta que este convencido de que tiene la cadena más larga, y obtener la rama de Merkele enlazando la transacción al bloque en el cual figura su timestamp. El usuario no puede chequear la transacción por si solo, pero si la enlaza a un lugar en la cadena,

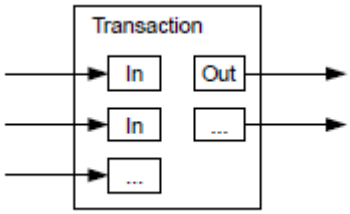
puede ver que un nodo de la red la aceptó, y los bloques siguientes confirman que la red la aceptó.



Como tal, la verificación es confiable mientras la red es controlada por nodos honestos, pero es más vulnerable si la red es dominada por un atacante. Mientras los nodos de la red pueden verificar las transacciones por ellos mismos, el método simplificado puede ser engañado por una transacción generada por un atacante, mientras el atacante domine la red. Una estrategia para protegerse contra eso sería aceptar alertas de nodos cuando detecten un bloque inválido, incitando al software del usuario a descargar el bloque completo y alertar transacciones para confirmar la inconsistencia. Los negocios que reciben pagos frecuentes probablemente querrán ejecutar sus propios nodos para obtener una mayor seguridad y una verificación más rápida.

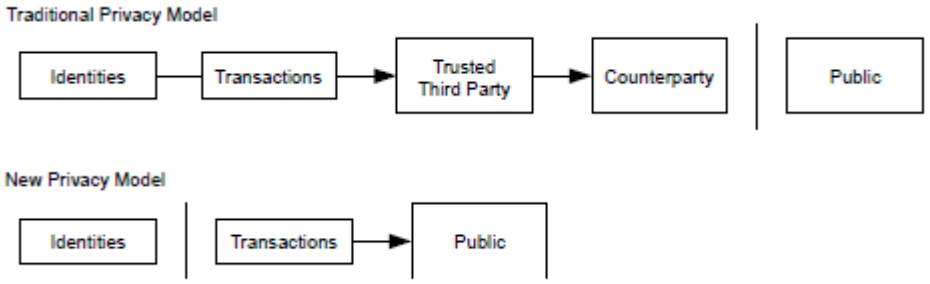
3.10 Combinación y división de valores

Aunque sería posible manejar a coins individualmente, sería pesado crear una transacción para cada centavo en una transferencia. Para permitir que un valor sea dividido y combinado, las transacciones contienen múltiples entradas y múltiples salidas. Normalmente habrá una entrada de una transacción mayor previa o entradas múltiples combinando valores menores, junto con dos salidas: una para el pago y otra para el vuelto, si es que lo hay, para el pagante.



3.11 Privacidad

El modelo de banca tradicional alcanza un nivel de privacidad limitando el acceso a información a las partes involucradas y la tercera parte de confianza. La necesidad de anunciar todas las transacciones públicamente imposibilita a este método, pero privacidad se puede alcanzar interrumpiendo el flujo de información en otra parte: manteniendo las claves públicas en anonimato. El público puede ver que alguien está enviando un monto a alguien, pero sin información enlazanda a nadie. Esto es similar al nivel de información publicado por las bolsas de valores, donde el tiempo y el tamaño del canje es abierto al público, pero sin contar quienes fueron las partes.



Como firewall adicional, para cada transacción debería utilizarse un par de claves diferente, para evitar que sean asociados a un usuario común. No se puede evitar un cierto nivel de asociación con transacciones de multi-entrada, las cuales necesariamente revelan que sus entradas fueron posesión del mismo dueño. El riesgo reside en cuando el dueño de una llave es revelado, se pueden descubrir otras transacciones relizadas por el mismo usuario.

4 Uso ilegal

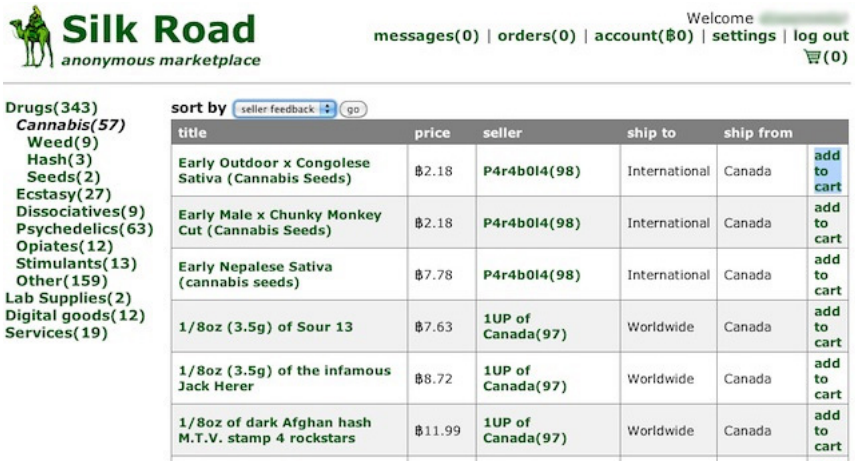
Un cyberesquema anarquista como Bitcoin rápidamente atrae a los cuatro jinetes del infocalipsis: La mafia, el tráfico de drogas, terroristas y la pornografá infantil. Desde que todas las transacciones son totalmente anónimas, Bitcoin se vuelve una herramienta muy poderosa para el lavado de dinero para la mafia. Grupos terroristas como Al Qaeda fácilmente pueden recibir soporte económico de forma segura utilizando bitcoins.
El grupo de hackers LulzSec (responsable por el hackeo de la páginas como la de Sony y del senado americano) recibió recientemente una donación de bitcoins por el valor de 7.000 dólares americanos.

Silk Road

Silk Road es un catálogo online de drogas que aceptaba bitcoins (y solo bitcoins) como forma de pago. El mismo fue cerrado el 5 de Junio del 2011. Tanto los vendedores como compradores son anónimos (de cualquier lado del mundo, la

mayoría de Canada y Estados Unidos) y se puede comprar cualquier tipo de droga que se pueda imaginar. Para facilitar las ventas, Silk Road empleaba un sistema de evaluación de los vendedores.

Acceder a Silk Road no es tan fácil. La url (`http://www.ianxz6zefk72ulzz.onion/index.php`) aparte de no ser amigable, tampoco es accesible de forma común mediante un browser. La única forma de acceder es mediante TOR: una red de encaminamiento *onion routing*, que permite a los usuarios comunicarse de forma anónima. La misma requiere habilidades técnicas para ser configurada.



Aunque no lo parezca a primera vista, Silk Road tiene límites: no permite la venta de artículos utilizados para dañar a otras personas, como armas de destrucción masiva, servicios de asesinato o tarjetas de crédito robadas.

Terrorismo doméstico

Para muchos (mandatarios americanos), establecer una moneda privada es terrorismo doméstico (ya que no involucra violencia). Sin embargo, hasta la guerra civil no existía moneda oficial en los Estados Unidos: los bancos emitían dinero en papel de forma totalmente legal. Lo que sí está prohibido por ley es crear una moneda privada basada en monedas metálicas. No existe una ley que prohiba una moneda privada.

5 El costo de generar bitcoins

Uno de los argumentos en contra de Bitcoin es la alta cantidad de energía utilizada para generar los bitcoins, la cual puede tener un valor monetario mayor al del misimo bitcoin generado. Esto quiere decir que si producimos bitcoins y los vendemos, no podríamos pagar la energía consumida para producirlos (al menos con precios de Estados Unidos).

Esto ayuda a evitar la inflación, ya que la cantidad de bitcoins que existirán es limitada (unos 21 millones).

Un argumento a favor del uso de tanta energía es que vale la pena consumirla para crear un sistema monetario libre. Se puede hacer una analogía a una minería de oro, que consume recursos para extraer el oro y transformarlo en barras.

Sin embargo, es un error común creer que el valor de un bitcoin es determinado por la cantidad de energía consumida para generarlo. El valor de un bitcoin es respaldado por el mercado: Los bienes y servicios que pueden ser adquiridos por los mismos.

Surge le pregunta: Porque el sistema no "suelta" los bitcoins de a poco en la red en vez de desperdiciar tantos recursos computacionales? La duda sería: A quien? Si se asignaran bitcoins a una billetera aleatoria, habrían mineros calculando trillones de direcciones (ya que cada usuario puede tener la cantidad de billeteras que se le antoje). Si se asignaran a una dirección IP aleatoria, se hubiera generado un crecimiento gigante en botnets y consumido gran parte de direcciones IPv6. Sin embargo, no se puede "mágicamente" simular poder computacional.

6 Usos

Aparte de los potenciales usos ilegales mencionados anteriormente, Bitcoin se utiliza para adquirar varios bienes y servicios totalmente legales, como hoteles, restaurantes, turismo, juegos, servicios profesionales (principalmente los orientados a web), software, música, revistas, etc. La mayoría se encuentra en los Estados Unidos y Europa. Algunos ejemplos a citar son:

1. Monarch Motel, Estados Unidos (`http://www.monarchmotel.com/`)
2. O'crepes, restaurante, Estados Unidos (`http://www.o-crepes.com/`)
3. Heidi Jo's Boutique, Estados Unidos (`http://www.heidijosboutique.com/`)
4. Rash Gash Guitars, Israel (`http://rashgash.co.il/`)
5. Musikhaus Shulte, tienda musical, Alemania (`http://www.realmusicshop.de/`)
6. Sanshinkai Aikido Utrecht, artes marciales, Holanda (`http://utrecht.sanshinkai.eu/`)

Una lista completa de páginas web que aceptan bitcoins como forma de pago se puede ver en `https://en.bitcoin.it/wiki/Trade` y un mapa de algunos locales que aceptan bitcoins como pago se puede ver en `https://en.bitcoin.it/wiki/Real_world_shops`. Una lista para América Latina se encuentra en `https://es.bitcoin.it/wiki/Comercio`.

7 Impacto social, económico y político

Bitcoin tiene la capacidad de cambiar el concepto de gobierno que manejamos hoy en día, debido a las siguientes razones: La moneda bitcoin no puede ser controlada por ninguna autoridad debido a su naturaleza descentralizada, mitigando posibles inestabilidades causadas por bancos centrales.

Bitcoin es no imponible (el gobierno no puede cobrar impuestos en las transacciones). Si Bitcoin algún día se transforma en la moneda standard de transacciones online, puede destruir al dinero fiduciario (dinero cuyo valor es dado por el estado). A esto se suma que las transacciones son totalmente anónimas, las cuales el estado no puede controlar. Los gobiernos probablemente tratarán de derrocar a Bitcoin, pero es poco probable que ocurra. En sintesis, el gobierno no tiene control sobre Bitcoin, como lo tiene con las monedas manejadas por los bancos. Al igual que Bittorrent, Bitcoin no es ilegal, pero se utiliza para actividades ilegales. Y sin embargo (tanto Bittorrent como Bitcoin) crecen diariamente.

Lo que le da tanto valor a Bitcoin son los principios de descentralización, apertura y pseudonimidad y tiene la capacidad de revolucionar la industria de pagos online y devolver el poder económico al pueblo.

8 Economía

La economía Bitcoin aún es pequeña y el software aún en estado beta, pero bienes y servicios reales (como por ejemplo automóviles y trabajos de programación) están siendo intercambiados. Los bitcoins son aceptados para servicios online o bienes tangibles. Se puede intercambiar bitcoins con monedas regulares, como el dólar americano y el euro.

La inflación no puede ser manipulada de forma centralizada, sino que el software Bitcoin controla la misma. El número de bitcoins tenderá a 21 millones con el tiempo. La oferta de dinero crece como una progresión geométrica a cada 4 (cuatro) años: en el 2013 la mitad de la oferta total habrá sido generada, en el 2017, 3/4 ya habrá sido generado. A medida que la cantidad de bitcoins llegue al límite, el valor de los bitcoin entrará en deflación. Los bitcoins son divisibles hasta 8 decimales, eliminando las limitaciones prácticas de los ajustes de precio en un ambiente deflacionário.

El último valor oficial de un BTC (Bitcoin) es de 4.1456 USD (9 de octubre del 2011) según el sitio Mt. Gox, uno de los principales centros de cambio entre

BTC y otras monedas como el USD o el euro (`https://mtgox.com/`). Es decir, en circulación están unos 32,726,100 USD. La cantidad total de BTC generados hasta la fecha son 7,437,750 BTC, según el sitio Bitcoin Watch, un sitio oficial que monitorea todas las actividades de la moneda (`http://www.bitcoinwatch.com/`).

Estos y más datos se pueden obtener siguiendo a la cuenta de twitter oficial `http://twitter.com/#!/bitcoineconomy`. El formato de cada tweet está explicado en `https://en.bitcoin.it/wiki/Bitcoin_Economy`.

El valor del BTC todavá está bastante fluctuante: En junio del 2011 un BTC tenía un valor aproximado de 30 USD (el valor más alto desde su creación), bajando a los 4 USD de octubre 2011. Más datos estadísticos se pueden obtener en `http://bitcoincharts.com`, mas específicamente en la sección charts.

En julio del 2011 el sitio Mt. Gox sufrió un ataque de hackers, lo que hizo que el precio descendiera a 1 centavo USD por un momento.

9 Posibles escenarios de fallo

Posibles motivos causantes de su fracaso son: la devaluación de la moneda, disminución de los usuarios, o una campaña gubernamental global en contra del software. Otro posible motivo de falla podría ser el caso que, los usuarios que actualmente ya poseen una cantidad elevada de bitcoins, y sabiendo que es una moneda en crecimiento, estén acumulando estos bitcoins, dado que el número total de bitcoins que alguna vez pueda existir es de 21 millones (al contrario del oro y el petróleo, para los cuales pueden encontrarse nuevas minas y depósitos). Sin embargo, siempre habrá alguien que gaste bitcoins y los ponga en circulación, pero se dará cuenta de que la mejor estrategia es acumularlos. Luego, el sistema fallará si nadie gasta los bitcoins para ponerlos en circulación. A esto se pueden agregar los bitcoins que no pueden circular: debido a usuarios que olvidaron de respaldar sus claves privadas, o usuarios que experimentaron en los inicios del sistema, generaron unos cuantos BTC y luego los dejaron en el olvido.

Otro peligro para Bitcoin es el caso en que muchos usuarios vendan todos sus bitcoins, generando una reacción en cadena, haciendo que el precio caiga al suelo (ya que hay más oferta que demanda de BTC).

10 Miners

Contrariamente a lo que se pueda pensar, la mayoría de los usuarios de Bitcoin no participan en la minería. Antiguamente la minerá de coins se hacía con la CPU, pero esto se fue sustituyendo por le minería a través de GPU, unas 50 a 100 veces más rápido. Si se desea minar una cantidad de BTC a cambio de cierto poder computacional, se puede firmar un *mining contract* como los listados en `https://en.bitcoin.it/wiki/Category:Mining_contractors`. Otra posibilidad es comprar harware diseado específicamente para la minería de bitcoins. Algunos se encuentran listados en `https://en.bitcoin.it/wiki/Category:`

Mining_Rig_Retailers. Hay dos maneras de realizar el mining: Una es participar de un mining pool, donde la ganancia total es dividida entre los participantes y por ende genera una ganancia estable, pero con algo de pérdida, ya que el administrador cobra un porcentaje como pago. La otra forma es minar de forma independiente, configurando un cliente Bitcoin (como se explica detalladamente en https://en.bitcoin.it/wiki/Running_Bitcoin) El miner GPU más popular al momento es el Python OpenCL Bitcoin Miner (poclbm - https://en.bitcoin.it/wiki/Poclbm). Otro miner es DiabloMiner, implementado en Java (https://en.bitcoin.it/wiki/DiabloMiner) Otra posibilidad (ilegal) es robar bitcoins a través de un malware, que se instala en máquinas con sistema operativo Windows y envía la billetera (un archivo .dat) por mail. Una solución a eso es encriptando la billetera.

11 Competitdores

Aparte de los competidores que adoptan el modelo centralizado (como PayPal y WebMoney), existen otros proyectos descentralizados (como Bitcoin). Uno de ellos es Ripple. Ripple es un proyecto de código abierto que se basa en una red social P2P con un sistema de honor monetario basado en confianza, parecido a redes sociales del mundo real (http://ripple-project.org/). Otro sistema parecido es Loom (https://loom.cc/), que puede ser utilizado para transferir cualquier título de posesión de forma privada. Su uso es más popular con el oro, dinero, plata, entre otros, pero puede utilizarse para cualquier tipo de propiedad.

12 Conclusiones

Para liberarse del sistema de transacciones centralizado en entidades financieras de confianza, se propuso un sistema para transacciones electrónicas sin necesidad de terceros de confianza. Para lograrlo, se planteó una red peer-to-peer utilizando proof-of-work para guardar el historial de transacciones que resulta prácticamente imposible de ser cambiado por un atacante en la red mientras los nodos honestos controlan la mayor parte de capacidad de CPU. La red es robusta y simple. Los nodos no necesitan identificarse ya que los mensajes no se rutean a ningun lugar concreto. Los nodos pueden entrar y salir de la red cuando quieran, aceptando la cadena proof-of-work como prueba de lo que sucedió mientras estuvieron ausentes. Los nodos votan con capacidad de CPU, expresando así la aceptación de bloques válidos con la expansión de la cadena y rechazando bloques inválidos, negando a expandirlos.

Esto le da a Bitcoin varias ventajas:

1. Se puede hacer una transacción de usuario a usuario directamente (sin necesidad de un banco)
2. Los honoriarios son mucho mas bajos
3. Se puede utilizar en cualquier país del mundo
4. La cuenta no puede ser congelada

5. No existen prerequisitos

Los bitcoins son generados en toda internet, por cualquier usuario ejecutando una aplicacción llamada minería de bitcoins. La generación de bitcoins requiere una cierta cantidad de trabajo para cada bloque de coins. Este monto se ajusta automáticamente por la red para que los bitcoins sean creados a una tasa constante. Los bitcoins se almacenan en una billetera digital. Al transferirse bitcoins, se agrega una firma digital. Esta transacción es luego verificada por un minero y luego se almacena permanentemente y anonimamente en la red. El software de Bitcoin es completamente open-source y cualquiera puede revisar el código. Esto lleva a que Bitcoin está cambiando al mundo de las finanzas, permitiendo el acceso al mercado a cualquier persona.

Hoy en día ya se pueden comprar videojuegos, regalos, libros, servidores y otras cosas con Bitcoins. Los bitcoins se pueden intercambiar con otras monedas como el Dólar o el Euro.

Todo esto conduce a que Bitcoin es una excelente opción para que pequeños negocios puedan entrar al mercado, ya que es gratis aceptar bitcoins, sin devoluciones de cargos y sin honoriarios.

Bitcoin puede generar grandes efectos colaterales: políticos, sociales y económicos, debido a que los gobiernos no pueden imponerlo ni controlarlo, ni mucho menos controlar quién compra qué cosa. Esto genera alteraciones entre los poderosos sectores polticos y bancarios.

13 Referencias

http://bitcoin.org.
http://en.wikipedia.org/wiki/bitcoin.
https://en.bitcoin.it/wiki/introduction.
http://www.technologyreview.com/computing/37619/?p1=a1&a=f.
http://www.weusecoins.com/.
Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
Dušan Barok. Bitcoin: censorship-resistant currency and domain name system to the people, 2011.
https://en.bitcoin.it/wiki/Myths
http://www.businessweek.com/magazine/content/11_26/b4234041554873.htm
http://www.businessweek.com/magazine/content/11_26/b4234041554873_page_2.htm
http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable
https://www.torproject.org/about/overview.html.en
https://bitcointalk.org/index.php?topic=4708.0
http://blogs.computerworld.com/18335/bitcoin_miners_busted_police_confuse_bitcoin_power_usage_for_pot_farm
http://xifin.wordpress.com/2010/11/18/bitcoin-a-rube-goldberg-machine-for-buying-electricity/
http://bitcoinweekly.com/articles/the-wasted-electricity-objection-to-bitcoin-part-i
https://en.bitcoin.it/wiki/Trade
https://en.bitcoin.it/wiki/Real_world_shops
https://es.bitcoin.it/wiki/Comercio
https://bitcointalk.org/index.php?topic=25829.0

http://www.investitwisely.com/bitcoin-the-digital-currency-of-the-future/
https://mtgox.com/
http://www.bitcoinwatch.com/
bitcoincharts.com
http://bitcoinweekly.com/articles/the-mtgox-attack
http://tav.espians.com/why-bitcoin-will-fail-as-a-currency.html
http://www.fredrikhallund.com/?p=344
http://memeburn.com/2011/05/will-bitcoin-be-another-failed-global-ecurrency/
http://www.weusecoins.com/mining-guide.php
http://www.wired.com/threatlevel/2011/06/bitcoin-malware/
http://www.zdnet.com/blog/security/new-bitcoin-malware-steals-bitcoin-wallets-infostealercoinbit/
8804
http://www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99&tabid=
2
http://en.wikipedia.org/wiki/Electronic_money
http://ripple-project.org/
https://loom.cc/