# Bitcoin

Priscilla Piedra y Martín Flores
Escuela de Ingeniería en Computación
Instituto Tecnológico de Costa Rica. Cartago, Costa Rica
{ppiedra90, mfloresg}@gmail.com

**Resumen**—

## 1. Introducción

LAS

## 2. Bitcoin

Bitcoin es una colección de conceptos y tecnologías que forma la base de un ecosistema monetario digital. La divisas llamada *bitcoin* se usa para almacenar y transmitir valor entro los participantes de una red bitcoin. Los usuario de bitcoin se comunican entre sí usando el protocolo bitcoin principalmente a través de Internet, aunque otras redes de transporte puede también ser usadas. Las tecnologías del protocolo bitcoin, disponibles como código abierto, puede ser ejecutadas en un amplio rango de dispositivos de computación, incluyendo computadoras portátiles y teléfonos inteligentes, haciendo que esta tecnología sea de fácil acceso.

Los usuarios pueden transferir bitcoins en una red para hacer básicamente cualquier cosa que puede ser heca con divisas convencionales, incluyendo la compra y venta de bienes, envío de dinero o para crédito. El bitcoin puede ser comprado, vendido e intercambiado por otras divisas con tipos de cambio especializados. En cierto sentido, bitcoin es la forma perfecta de dinero para el Internet porque es rápida, segura y sin fronteras.

A diferencia de divisas tradicionales, los bitcoins son totalmente virtuales. No hay monedas físicas o monedas digitales como tal. Las monedas están implícitas en transacciones que transfieren valor desde un emisor hacia un destinatario. Los usuarios de bitcoin tienen llaves que les permite probar la propiedad de un bitcoin en una red bitcoin. Con estas llaves puede firmar transacciones para desbloquear/liberar el valor y gastarlo al trasferirlo a un nuevo dueño. Las llaves son usualmente almacenadas en un monedero digital en la computadora o dispositivo de cada usuario. La poseción de una llave que pueda firmar una transacción es sólo el prerequisito para gastar bitcoins, se da el control total a los usuarios.

El bitcoin es un sistema distribuido punto-a-punto. Como tal no hay un servidor "central" o un punto de control. Los bitcoins son creado a través de un proceso llamado minería (*minning*) el cual involucra competir para encontrar soluciones a un problema matemático mientras se procesa la transacción bitcoin. Cualquier participante de la red bitcoind (por ejemplo, cualquiera usando un dispositivo que corre el conjunto total del protocol bitcoin) puede operar como minero, usado el poder de procesamiento de su computadora para verificar y guardar transacciones. Cada 10 minutos, en promedio, un minero bitcoin es capaza de validar las transacciones de los 10 minutos pasados y se le premia con un nuevo bitcoin. Esencialmente, la minería de bitcoins descentraliza la emisión de moneda y otras funciones de un banco central y reemplaza la necesidad de tener uno.

El protocolo bitcoin incluye algoritmos que regulan la función de minería a través de la red. La dificultad de la tarea de procesamiento que los mineros deben realizar se ajusta dinámicamente así, en promedio, alguien tiene éxito cada 10 minutos independientemente de cuántos mineros (y qué tanto procesamiento) están compitiendo en algún momento. Cada 4 años, el protocolo también reduce a la mitad la proporción en la que un nuevo bitcoin es creado, y limita el número total de bitcoin que podrían ser creado a un total fijo por debajo de 21 millones de monedas. El resultado es que el número de bitcoin en circulación sigue una curva predecible que se acercará a 21 millones para el año 2140. Debido a la disminución de la tasa de emisión de Bitcoin, a largo plazo, la moneda de Bitcoin es deflacionista. Además, bitcoin no puede ser inflada "imprimiendo" nueva moneda por encima o por debajo del índice esperado de emisión.

Detrás de escenas, bitcoin es también el nombre del protocolo, una red punto-a-punto. La divisa bitcoin es realmente sólo la primer aplicación de esta invención. Bitcoin representa la culminación de décadas de investigación en criptografía y sistemas distribuidos e incluye cuatro innovaciones claves que se unen de una forma única y poderosa. Bitcoin consiste de:

- Una red descentralizada punto-a-punto (el protocolo bitcoin)
- Una libro de transacciones públicas (blockchain)
- Un conjunto de reglas para validación de transacciones y emisión de divisas (reglas de concenso)
- Un mecanismo para alcanzar consenso descentralizado global en un blockchain válido (algoritmo de prueba de trabajo[1])

*Este documento fue realizado durante el curso Redes de Computadoras Avanzadas, impartido por el profesor Luis Carlos Loaiza Canet. Programa de Maestría en Computación, Instituto Tecnológico de Costa Rica. Segundo Semestre, 2017.*

1. *Proof-of-Work Algorithm*

### 2.1. Historia

Bitcoin fue inventado en el 2008 con la publicacio4n de un artículo titulado *"Bitcoin: A Peer-to-Peer Electronic Cash System"* escrito bajo el álias de Satoshi Nakamoto. Nakamoto combinó varias invenciones previas como b-money y HashCash para crear un sistema de efectivo electrónico completamente descentralizado que no depende de una autoridad central para emisión de divisas o liquidacio4n y validación de transacciones. La innovación clave fue usar un sistema de computación distribuida (llamado el algoritmo de prueba de trabajo) para conducir una "elección" global cada 10 minutos, permitiendo a la red descentralizada lograr un consenso acerca el estado de transacciones. Esto resuelve elegantemente el problema del doble-gasto en donde una sola unidad en una divisa podía ser gastada dos veces. Previamente, el problema del doble-gasto fue una debilidad de las divisas digitales y fue abordado limpiando todas las transacciones a través de una "casa de limpieza" central.

La red bitcoin inició en el 2009, basado en una implementacio4n de referencia publicada por Nakamoto y desde ese momento revisada por muchos otros programadadores. La implementación del algoritmo de prueba de trabajo (minería) que proporciona seguridad y resiliencia para bitcoin ha incrementado su poder exponencialmente, y ahora excede la poder de procesamiento combinado de las principales supercomputadoras del mundo. El valor total de mercado de Bitcoin ha excedido en ocasiones los $35 millones, dependiendo de la tasa de intercambio bitcoin-a-dólar. Las transacción más grande procesada hasta ahora por la red fue $150 millones transmitidos instantaneamente y procesada sin ninguna comisión.

Satoshi Nakamoto se retiró del público en abril del 2011, dejando la responsabilidad de desarrollo del código y la red a un grupo de voluntarios. La identidad de la persona o personas detrás de bitcoin aún se desconoce. Sin embargo, ni Satoshi Nakamoto o alguien más ejerce control individual sobre el sistema bitcoin, el cual opera basado en principios matemáticos transparentes, código abierto y consenso entre los participantes. La invención como tal es pionera y se ha engendrado nueva ciencia en los campos de computación distribuida y economía.

### 2.2. Iniciando con Bitcoin

Bitcoin es un protocolo que puede ser accesado usando un aplicación cliente que hable el protocolo. Un "monedero bitcoin" es la interfaz de usuario más común con el sistema bitcoin. Existen varias implementaciones y marcas de monederos bitcoin, varían en calidad, rendimiento, seguridad, privacidad y confiabilidad. Está también la implementación de referencia del protocolo bitcoin que incluye un monedero conocido como el "Satoshi Client" o "Bitcoin Core", que se deriva de la implementación original escrita por Satoshi Nakamoto.

#### *2.2.1. Obteniendo el primer Bitcoin*

La primer y más difícil tarea para los nuevos usuarios es adquirir algún bitcoin. A diferencia de otras divisas extranjeras, no se puede comprar aún bitcoin en un banco o en un kiosko de intercambio de divisas.

Las transacciones de bitcoins son irreversibles. La mayoría de redes de pago como tarjetas de crédito, débito, PayPal y cuentas de banco son reversibles. Para alguien que vende bitcoin, esta diferencia introduce un riesgo muy alto de que el comprador revierta el pago electrónico después de haber recibido bitcoin, en efecto defraudando al vendedor. Para mitigar este riesgo, compañías que aceptan pagos electrónicos tradicionales en retorno de bitcoin usualmente le solicitan a los compradores pasar por verificaciones de identidad y crédito que puede tomar días o semanas. Como nuevo usuario, esto significa que no se puede comprar bitcoin instantaneamente con una tarjeta de crédito. Algunos métodos para obtener bitcoins como nuevo usuario son:

- Buscar un amigo que tenga bitcoin y comprarle algunos directamente.
- Usar un servicio clasificado como localbitcoins.com para encontrar vendedores y comprar bitcoin en una transacción en persona.
- Se puede ganar bitcoins por medio de la venta de un producto o servicio.
- Utilizar un ATM de bitcoin que acepte efectivo y envíe bitcoins a un monedero.

## 3. ¿Cómo funciona Bitcoin?

El sistema bitcoin, a diferencia de sistemas de banca y pagos tradicionales, está basado en confianza descentralizada. En lugar de una autoridad central de confianza, en bitcoin, la confianza se logra como una propiedad emergente de las interacciones de diferentes participantes en el sitema bitcoin.

En la figura 1 se ve que el sistema bitcoin conside de usuarios con monederos que contienen llaves, transacciones que son propagadas a través de la red y mineros que producen (a través de computación competitiva) el *consensus blockchain*, que es el libro de mayor autoridad de todas las transacciones.

### 3.1. Transacciones Bitcoin

En términos simples, una transacción le dice a la red que el propietario de algún valor de bitcoin ha autorizado la transferencia de ese valor a otro propietario. El nuevo propietario puede ahora gasta el bitocoin creando una nueva transaccio4n que autoriza transferir a otro propietario y así sucesivamente, en una cadena de propiedad.

#### *3.1.1. Entradas y Salidas de la Transacción*

Las transacciones son como líneas en un libro de contabilidad de doble entrada [2]. Cada transacción contiene una o mas "entradas", que son como débitos contra una cuenta bitcoin. En el otro lado de la trasacción, hay una o más "salidas", que son como créditos agregados a una cuenta bitcoin. Las entradas y salidas (débitos y créditos) no necesariamente suman la misma cantidad. Las salidas se suman a un poco menos que las entradas y la diferencia representa una tarifa de transacción implícita, que es un pequeño pago cobrado por el minero que incluye la transacción en el libro mayor. Una transacción bitcoin se muestra como un libro de contailidad en la figura 2.

2. *Double-entry bookkeeping ledger*

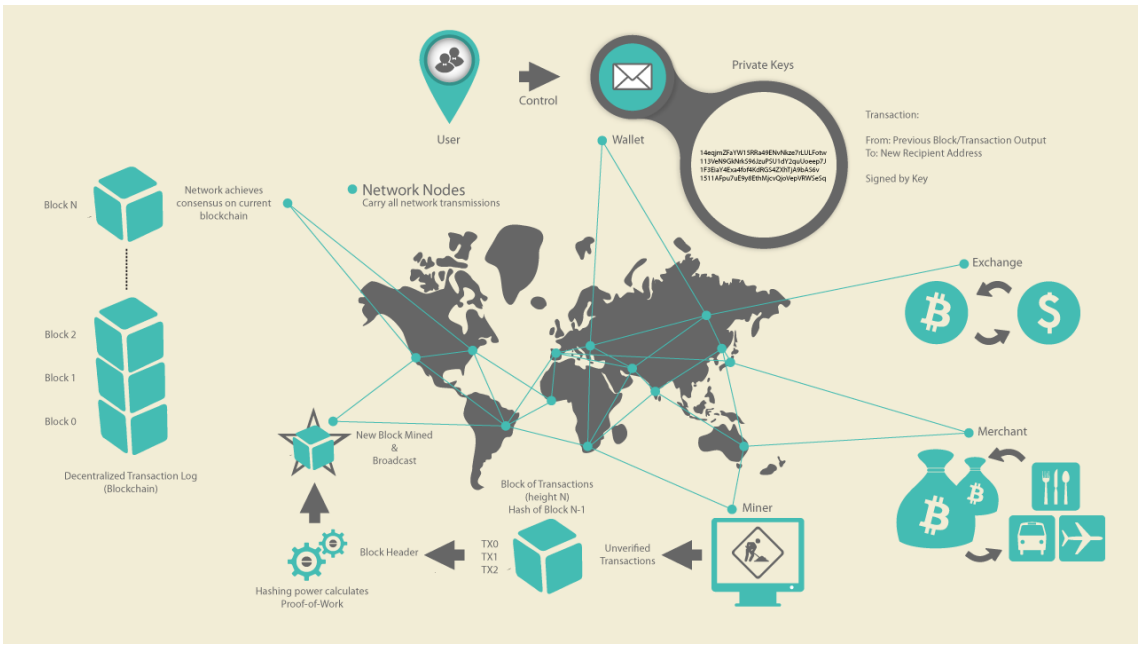


Figura 1. Bitcoin: visión general. citerexford.

La transacción también contiene pruebas de propiedad para cada cantidad de bitcoin (entradas) cuyo valor se está gastando, en forma de una firma digital del propietario, que puede ser independientemente validado por cualquiera. En términos bitcoin, "gastar" es firmar una transacción que transfiere el valor de una transacción anterior a un nuevo propietario identificado por una dirección de bitcoin.

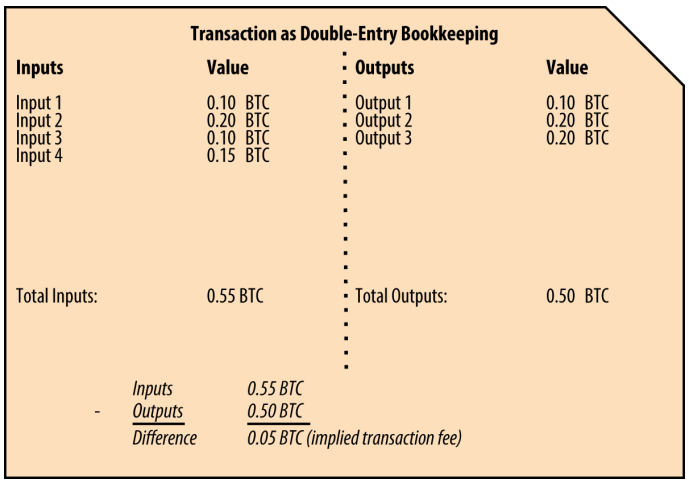


Figura 2. Transacción Bitcoin vista como un libro de contabilidad. citerexford.

### 3.1.2. *Cadenas de transacciones*

Un pago usa la salida una transacción previa como su entrada. Las transacciones forman una cadena, en donde las entras de la última transacción corresponden a la salida de transacciones previas. La llave de un usario proporciona la firma que libera esas transacciones previas, probando así a la red bitcoin que el usuario es dueño de los fondos. Una cadena de transacciones se muestra en la figura 3

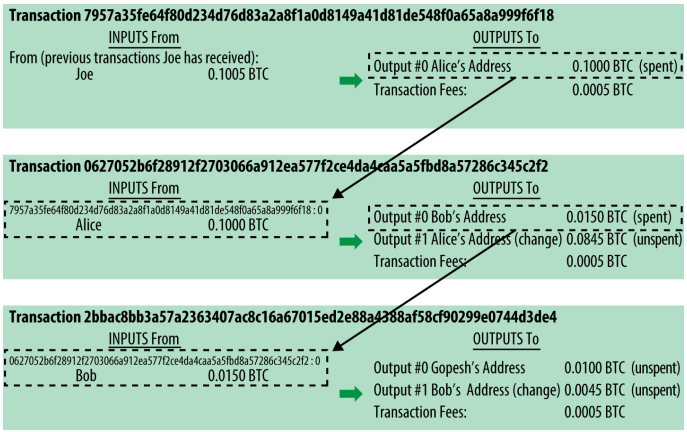


Figura 3. Una cadena de transacciones, donde la salida de una transacción es la entrada de la otra. citerexford.

Muchas transacciones bitcoin incluyen salidas que referencias ambos, una dirección del nuevo propietario y una dirección del propietario actual, llamada la *change address*. Esto es porque las entradas de la transacción no pueden ser divididas. Si se compra un artículo de $5 en una tienda pero se usa un billete de $20 para pagarlo, se espera recibir $15 como cambio. El mismo concepto aplica con las entradas de transacción en bitcoin. Si se compra un artículo que cuesta 5 bitcoins pero solo se tiene 20 bitcoins para usar, se enviaría una salida de 5 bitcoin al propietario de la tienda y una salida de 15 bitcoin de vuelta al usuario como cambio (menos cualquier comisión de transacción aplicable). El *change address* no tiene que tener la misma dirección que la que se usó como entrada y por razones de privacidad es usualmente una nueva dirección del monedero del propietario.

En resumen, las transacciones mueven valir desde entradas de transacción a salidas de transacción. Una entrada es una referencia a una salida de transacción previa, que

muestra de donde viene el valor. Una salida de transacción direcciona un valor específico a una nueva dirección de propietario bitcoin y puede incluer una salida de cambio de vuelta al propietario original. Las salidas de una transacción pueden ser usadas como entras en una nueva transacción, creando así una cadena de propiedad conforme el nuevo valor se muee de un propietario a otro.

## 4. Conclusión

## Referencias

[1] S. Nakamoto. *Bitcoin:A Peer-to-Peer Electronic Cash System*. Que. www.bitcoin.org

**Priscilla Piedra** es Ingeniera de Computación del Tecnologíco de Costa Rica. Actualmente es estudiante del programa de Maestría en Ciencas de la Computación en la misma universidad. Sus principales intereses son: *cloud computing* y automatización.


**Martín Flores** es Ingeniero en Informática de la Universidad Nacional. Actualmente, realiza sus estudios de Maestría en Ciencias de la Computación del Tecnológico de Costa Rica. Sus principales intereses son: lenguajes de programación, ingeniería de software y *DevOps*.