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

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])

1.1. Historia

Bitcoin fue inventado en el 2008 con la publicacio4n de un artículo titulado *"Bitcoin: A Peer-to-Peer Electronic Cash*

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*

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.

1.2. 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.

1.2.1. 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.

2. ¿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.

2.1. 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.

2.1.1. 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.

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

2. *Double-entry bookkeeping ledger*

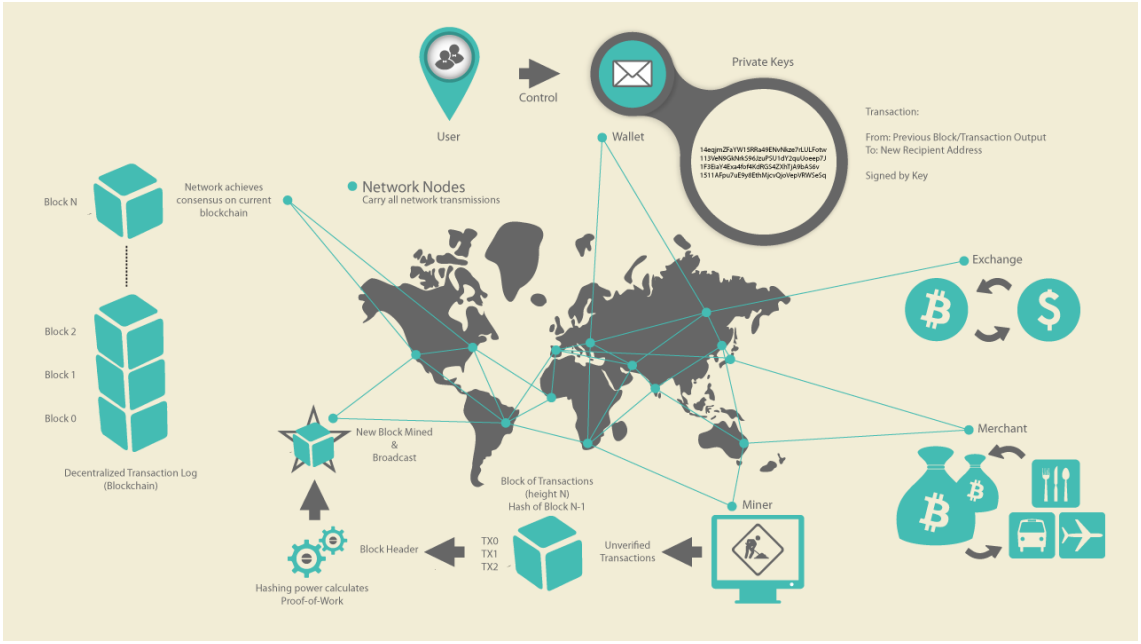

Figura 1. Bitcoin: visión general

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.

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

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

2.1.2. *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

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

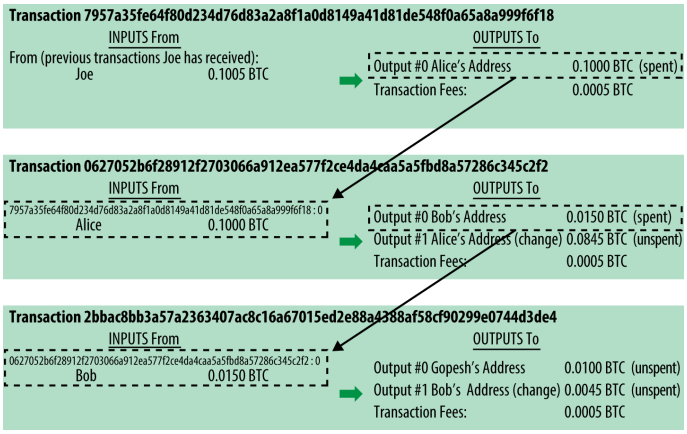

Figura 3. Una cadena de transacciones, donde la salida de una transacción es la entrada de la otra.

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 mueve de un propietario a otro.

2.2. Formas comunes de transacción

La forma más comurn de transaccio4n es un pago simple desde una dirección a otra, la cual usualmente incluye algun "cambio" retornado al propietario original. Este tipo de transacción tiene una entrada y dos salidas como se muestra en la figura 4

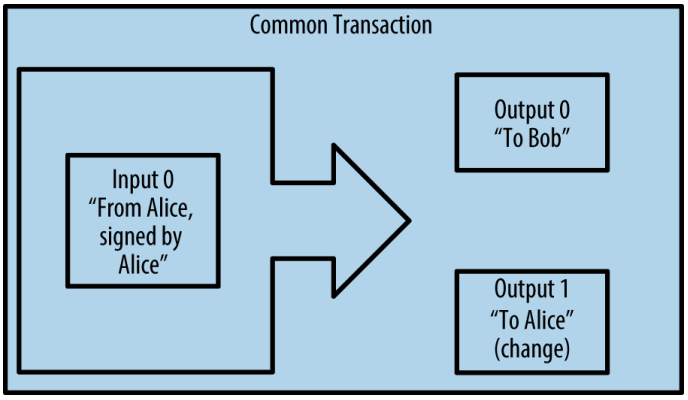

Figura 4. La transacción más común

Otra forma común de transacción es una que agrega varias entradas en una sola salida. Esto representa el equivalente en el mundo real a cambiar una pila de monedas y billetes por una sola nota. Transacciones como estas son algunas veces generadas por aplicaciones de monedeors para limpiar muchos pequeños montos que fueron recibidos como cambio de pagos previos.

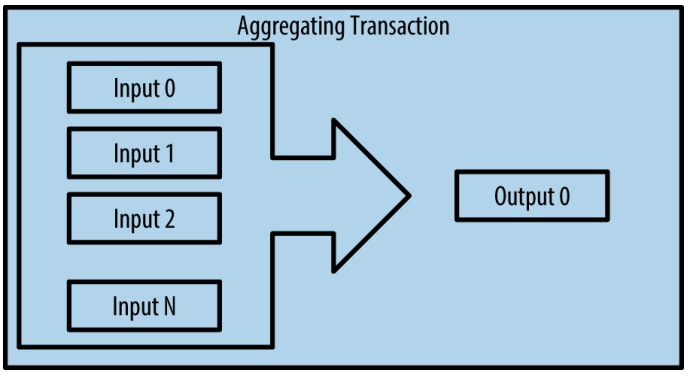

Figura 5. Transacción de fondos agregados

Finalmente, otra forma de transacción que se ve con frecuencia en el libro de bitcoin es una transacción que distribuye una entrada en varias salidas representando múltiples destinatarios. Este tipo de transacción la usan a veces las entidades comerciales para distribuir fondos, como cuando se procesa el pago de la nómina a múltiples empleados.

2.3. Construyendo una Transacción

La aplicación de monedero de un usuario contiene toda la lógica para seleccionar las entradas y salidas apropiadas para construir una transacción. El usuario sólo necesita

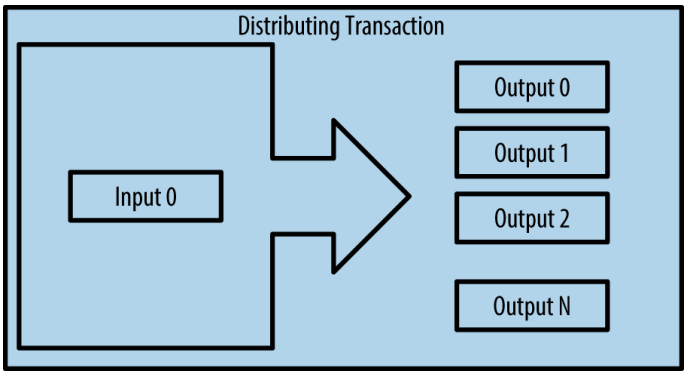

Figura 6. Transacción de fondos distribuidos

especificar un destino y un monto y el resto sucede en la aplicación de monedero sin que se vean los detalles. La aplicación de monedero puede construir transacciones inclusive cuando esta totalmente fuera de línea. Tal y como escribir un cheque en la casa y enviarlo luego al banco, la transacción no necesita que se construya y se firme mientras se está conectado a la red bitcoin.

2.3.1. *Obteniendo las entradas apropiadas*

La aplicación de monedero primer tiene que buscar las entradas para que pueda pagar la cantidad deseada. La mayoría de los monederos llevan un registro de toas las salidas disponibles que pertenecen a la dirección del monedero. Una aplicación de monedero que se ejecute como *full-node client* contiene una copa de todas las salidas pendientes para cualquier transacción en el blockchain. Esto permite que el monedero construya entradas de transacciones y verifique rápidamente que las transacciones entrantes tengan entradas correctas. Sin embargo, debido a que un *full-client node* ocupa mucho espacio en disco, la mayoría de los usuarios de monederos usan la versión "liviana" que solo registra las salidas no utilizadas del usuario.

Si la aplicación de monedero no mantiene una copia de las transacciones pendientes, puede entonces hacer una consulta a la red bitcoin para obtener esta información usando una variedad de API[3] disponibles por diferentes proveedores o preguntando a un *full-node* usando una llamada por programación.

2.3.2. *Creando las salidas*

Una salida de transacción se crea en forma de un script que crea un gravamen en el valor y solo se puede canjear mediante la introducción de una solución al script. En términos simples, la salida de la transacción de un usuario A va contener un script que dice algo como "Esta salida se paga a quien pueda presentar una firma desde la llave correspondiente a la dirección pública de B, siendo B en este caso el destinatario de la transacción. Debido a que sólo el usuario B tiene el monedero con las llaves correspondientes a esa dirección, solamente el monedero de B puede presentar dicha firma para redimir esta salida. Por lo tanto, A "gravará" el valor de la salida con una demanda de una firma de B.

3. *Application Programming Interface*

Finalmente, para que la transacción pueda ser procesada por la red de manera oportuna, la aplicación de monedero de A agregará una pequeña comisión. La comisión de transacción que colecta el minero es una tarifa para validar e incluir la transacción en un bloque que se registrará en el blockchain.

2.3.3. Agregando la transacción al libro

La transacción anteriormente cread contiene ahora todo lo necesairo para confirmar la origen de los fondos y asignar nuevos propietarios. Ahora la transacción debe ser transmitida a la red bitcoin donde será parte del blockchain.

2.3.3.1. Transmitiendo la transacción: debido a que la transacción contiene toda la información necesario para procesarse, no importa cómo o dónde se transmite en la red bitcoin. La red bitcoin es una red punto-a-punto, en donde cada cliente bitcoin participa al conectarse con otros clientes bitcoin. El propósito de la red bitcoin es propagar transacciones y bloques a todos los participantes.

2.3.3.2. ¿Cómo se propaga?: Cualquier sistema, como un servidor, aplicación o monedero que participa en la red bitcoin al "hablar" el protocolo bitcoin se llama un nodo bitcoin. La aplicación de monedero de un usuario puede enviar la nueva transacción a cualquier nodo bitcoin. El monedero no necesita esta conectado directamente al monedero de otro usuario tampoco.Cualquier nodo bitcoin que reciba una transacción válida que no se haya visto antes lo reenviará inmediatamente a todos los otros nodos a los que esté conectado, una técnica de propagación conocida como inundación (*flooding*). Así, la transacción se propaga rápidamente a través de la red punto-a-punto, alcanzando un gran porcentaje de los nodos en unos pocos segundos.

3. Minando Bitcoin

Una transacción que se propaga a través de la red bitcoin no se convierte en parte del blockchain hasta que sea verificada e incluida en un bloque por un proceso llamado minería (*minning*).

El sistema de confianza de bitcoind está basado en computación. Las transacciones se agrupan en bloques, que requieren una gran cantidad de cómputo para probar, pero solo una pequeña cantidad de cómputo para verificarlo como comprobado. El proceso de minería tiene dos propósitos en bitcoin:

- Los nodos de minería validan todas las transacciones con referencia en las reglas de consenso de bitcoin. Por lo tanto, la minería proporciona seguridad para las transacciones bitcoin al rechazar transacciones inválidas o mal formadas.
- La minería crea un nuevo bitcoin en cada bloque, casi como un banco central imprime nueva moneda. La cantidad de bitcoin creado por bloque es limitado y disminuye con el tiempo, siguiendo un calendario de emisión fijo.

La minería logra un fino equilibrio entre los costos y la reconmpensa. La minería usa electricidad para resolver un problema matemático. Un minero exitoso va a recolectar una recompensa en la forma de nuevos bitcoins y comisiones de transacciones. Sin embargo, la recompensa solamente será recolectada si un minero ha validado correctamente todas las transacciones, para satisfacer las reglas de concenso. Este delicado balance proporciona seguridad para bitcoin sin una autoridad central.

Una buena forma para describir la minería es como un gigante juego competitivo de sudoku que se reinicia cada ver que alguien encuentra una solución y cuya dificultad automáticamente se ajusta para que tome aproximadamente 10 minutos para encontrar la solución. Este juego gigante de sudoku se puede imaginar con un tamaño de miles de columnas y filas. Si se muestra que el juego fue resuelto se puede verificar rápidamente. Sin embargo, si el juego tiene varios cuadros llenos y varias vacíos, tomará mucho trabajo en ser resuelto. La dificultad del sudoku puede ser ajustada al cambiar su tamaño (más o menos filas y columnas), pero aún asi puede ser verificado fácilmente. El "juego" usado en bitcoin se base en una función *hash* criptográfica y expone características similares: es asimétricamente difícil de resolver pero fácil de verificar, y esta dificultad puede ser ajustada.

4. Minando Transacciones en Bloques

Nuevas transacciones están constantemente fluyendo dentro de la red desde monederos de usuarios y otras aplicaciones. Como estos son vistos por la red bitcoin como nodos, se agregan a un *pool* temporal de transacciones no verificadas mantenidas por cada nodo. Conforme los mineros construyen un nuevo bloque, van agregando transacciones no verificadas desde este *pool* a un nuevo bloque y luego intentan probar la validez de ese nuevo bloque, con el algoritmo de minería de prueba-de-trabajo.

Las transacciones son agregadas a un nuevo bloque, priorizadas de acuerdo con las comisiones de transacción más altas y alguna otros criterios. Cada minero inicia el proceso de minería de un nuevo bloque de transacciones tan pronto y como recibe un bloque previo de la red, a sabiendas que a perdido la ronda previa de competición. Inmediatamente crea un nuevo bloque, lo llena con las transacciones y una huella (*fingerprint*) del bloque previo, e inicia el cálculo de la prueba-de-trabajo para el nuevo bloque. Canda minero incluye una transacción especial a su bloque, uno que paga su propia dirección de bitcoin la recompensa del bloque más la suma de comisiones de trasacción de todas las transacciones incluidas en el bloque. Si encuentra una solución que haga que ese bloque sea válido, él "gana" su recompensa porque su bloque exitoso se agregó al blockchain global y la transacción de recompensa que él incluyó se vuelve en gastable.

4.1. Ejemplo: Jing y Alice

Jing es un usuario que lleva varios años participando del proceso de minería. Ha configurado su software para crear nuevos bloques que asignas un premio al *pool* de direcciones. A partir de ahi, una parte del premio es distribuido a Jing y a otros mineros en proporción a la cantidad de trabajo con el que contribuyan en la última ronda.

Alice ha realizado una transacción y esta ha sido tomada por la red e incluida en un *pool* de transacciones no verificadas. Una vez validada por el software de minería fue

incluida en un nuevo bloque, llamado bloque candidato, generado por el *pool* de minería de Jing. Todos los mineros participando en ese *pool* de minería inician inmediatamente el cálculo de la prueba-de-trabajo para el bloque candidato. Aproximadamente cinco minutos después que la transacción fue transmitida por el monedero de Alice, uno de los circuitos de minería de Jing encuentra la solución para el bloque candidato y lo anuncia a la red. Mientras que los otros mineros valida el bloque ganador, ellos inician la carrera para generar el próximo bloque.

El bloque ganador de Jing se vuelve parte del blockchain como el bloque #277316, que contiene 420 transacciones, incluyendo la transacción de Alice. El bloque que contiene la transacción de Alice se cuenta como una "confirmación" de esa transacción.

Aproximadamente 19 minutos después, un nuevo bloque #277317, es minado por otro minero. Debido a que este nuevo bloque está construido por encima del bloque #277316 que contiene la transacción de Alice, se añade aun más computación al blockchain, por lo tanto fortalece la confianza en esas transacciones. Cada bloque minado sobre el que contiene la transacción cuenta como una confirmación adicional para la transacción de Alicia. Conforme los bloques se apilan uno por encima del otro, se vuelve exponencialmente más difícil reversar la transacción, de esta forma se hace más y más confiable por la red.

En la figura 7, se puede ver el bloque #277316, que contiene la transacción de Alice. Por debajo hay 277316 bloques (incluyendo el bloque #0), enlazados unos con otros en una cadena de bloques (blockchain) hasta regresar al bloque #0, conocido como el bloque genesis. Con el tiempo, conforme la "altura" en bloques aumentaa, también lo hace la dificultad de calcular cada bloque y la cadena como un todo. Los bloques minados luego del que contiene la transacción de Alice actúan como una garantía adicional, ya que acumulan más cómputos en una cadena cada vez más larga. Por convención cualquier bloque con más de seis confirmaciones es considerado irrevocable, porque va a requerir una inmensa cantidad de computación para invalidar y recalcular seis bloques.

4.2. Gastando la Transacción

Ahora que la transacción de Alice ha sido agregada en el blockchain como parte de un bloque, es parte de un libro distribuido de bitcon y es visitble a todas las aplicaciones bitcoin. Cada cliente bitcoin puede verificar independientemente la transacción y considerarla válida para gastar. Los clientes *full-node* pueden rastrear el origien de los fondos desde el momento en que el bitcoin fue generado en un bloque, de forma incremental, transacción a transacción, hasta que llegue a la dirección de un destinatario. Los clientes "livianos" pueden hacer lo que se llama un verificación de pago simplificada al confirmar que la transacción está en el blockchain y tiene varias bloques minados despues de ella, lo que garantiza que los mineros la aceptaron como válida.

El destinatario de los fondos puede ahora gastar la salida de la transacción y conforme recibe pagos de otros, él a su vez extiende la cadena de transacciones. Un ejemplo de esta cadena de transacciones agregadas se puede ver en la figura 8

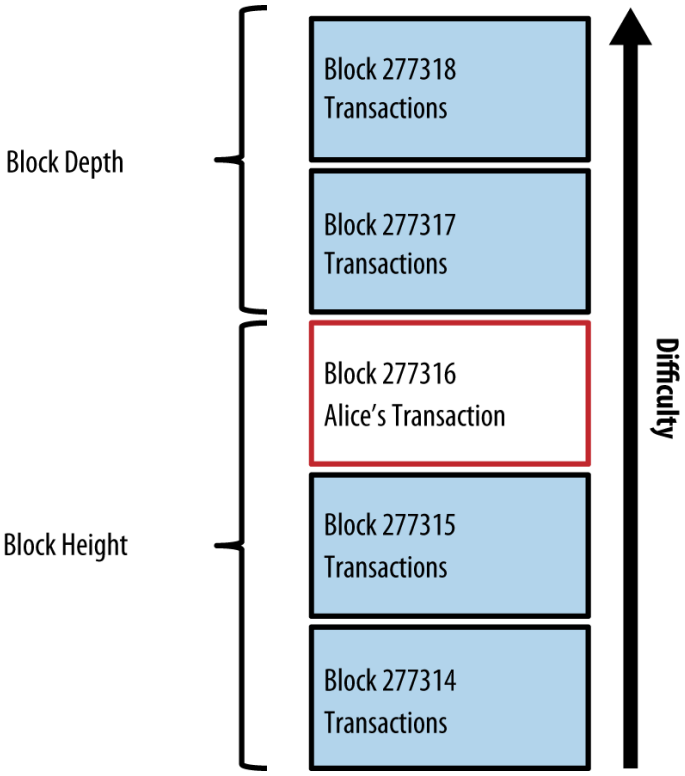

Figura 7. Transacción de fondos agregados

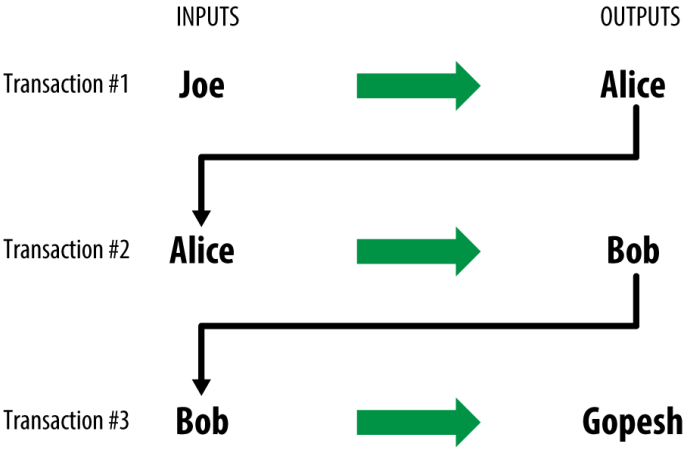

Figura 8. Las transacciones de Alice como parte de una cadena de transacciones de Joe hasta Gopesh

5. Conclusión

Referencias

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

[2] A M. Antonopoulos. *Mastering Bitcoin* . Segunda Edición. O'Reilly Media, Inc. ISBN: 9781491954386. Junio 2017.

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*.