CUADERNOS CEF / N° 1

Estudio sobre Bitcoin y Tecnología Blockchain

HÉCTOR ACUÑA

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

NOVIEMBRE | 2017

Estudio sobre Bitcoin y Tecnología Blockchain

HÉCTOR ACUÑA / contacto: hacuna.ese@uandes.cl[1]

Noviembre 2017

Resumen

La integración financiera europea, la reciente crisis económica y financiera, y el amplio desarrollo digital, han transformado profundamente el sector monetario y el mercado de comercio electrónico. Un claro ejemplo de estos cambios es la creación de monedas virtuales como el Bitcoin, que viene a ser una alternativa al sistema monetario tradicional.

Bitcoin surge como una solución a la necesidad de los usuarios de un intercambio mundial facilitado por herramientas de pago transnacionales, y que a menudo se traduce en la voluntad de liberarse de los actores tradicionales de los circuitos monetarios.

En 2008 se origina este sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiendo que dos partes interesadas realicen transacciones directamente sin la necesidad de una tercera parte confiable. Este sistema dio origen a la criptomoneda Bitcoin y la tecnología con la que opera se denominó *blockchain* o cadena de bloques.

En este trabajo se presenta una completa revisión de la tecnología *blockchain*, de sus principales elementos y características, y su funcionamiento detrás de Bitcoin. Luego, se discute sobre los desafíos en el ámbito regulatorio que conlleva el uso de la criptomoneda, y en torno al impacto potencial de Bitcoin en los mercados financieros locales. Finalmente, se realiza una breve descripción sobre las aplicaciones potenciales de la tecnología *blockchain* a distintas operaciones en los mercados globales.

[1] Investigador del Centro de Estudios Financieros - ESE Business School de la Universidad de Los Andes. Email: hacuna.ese@uandes.cl. Agradezco los valiosos comentarios de M. Cecilia Cifuentes y J. Gabriel Fernández. Cualquier error u omisión es de mi exclusiva responsabilidad.

Contenido

1. Introducción

La integración financiera europea, la reciente crisis económica y financiera, y el amplio desarrollo digital, han transformado profundamente el sector monetario y el mercado de comercio electrónico. Un claro ejemplo de estos cambios es la creación de monedas virtuales como el Bitcoin, que viene a ser una alternativa al sistema monetario tradicional.

El comercio en internet ha llegado a depender casi exclusivamente de las instituciones financieras, las cuales sirven como terceras partes de confianza (ministros de fe de las operaciones), para el procesamiento de los pagos electrónicos.

Bitcoin surge como una solución a la necesidad de los usuarios de un intercambio mundial facilitado por herramientas de pago transnacionales, y que a menudo se traduce en la voluntad de liberarse de estos actores tradicionales de los circuitos monetarios.

Lo anterior se da debido a que mientras el sistema tradicional funciona razonablemente bien para la mayoría de las transacciones, aún padece de las debilidades inherentes de los modelos basados en confianza. Las transacciones completamente irreversibles no son realmente posibles, debido a que las instituciones financieras no pueden evitar la mediación en ciertas disputas. El costo de mediación incrementa los costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de realizar pequeñas transacciones casuales, sumando esta limitación a la imposibilidad de hacer pagos irreversibles por servicios que también lo son.

Con la posibilidad de revertir una transferencia, la necesidad de confianza se incrementa. Los comerciantes deben tener precaución al elegir a sus clientes y solicitarles más información de la que se necesitaría en un sistema de transacciones irreversibles.

A raíz de los inconvenientes mencionados, en 2008 se origina este sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiendo que dos partes interesadas realicen transacciones directamente sin la necesidad de una tercera parte confiable. Este sistema dio origen a la criptomoneda Bitcoin y la tecnología con la que opera se denominó *blockchain* o cadena de bloques.

En este trabajo se presenta una completa revisión de la tecnología *blockchain*, de sus principales elementos y características, y de su funcionamiento detrás de Bitcoin. En la sección 2 se presenta una breve revisión de la literatura. En la sección 3 se presenta el concepto de Bitcoin y su irrupción en el mercado de comercio electrónico. Luego, para lograr un mayor entendimiento del sistema, en la sección 4, se presenta una breve descripción de cómo funciona el sistema tradicional de transferencias bancarias para luego, en la sección 5, adentrarse en el estudio de esta nueva tecnología. En la sección 6 se presenta la aplicación de la tecnología *blockchain* a las operaciones con Bitcoin. En la sección 7 se realiza una breve comparación entre el sistema tradicional y el sistema con tecnología *blockchain*. En la sección 8 se discute sobre los desafíos en el ámbito regulatorio que conlleva el uso de la criptomoneda, mientras que en la sección 9 se discute sobre el impacto potencial de Bitcoin en los mercados financieros locales. En la sección 10 se realiza una breve descripción sobre las aplicaciones potenciales de la tecnología *blockchain* y, finalmente, la sección 11 presenta las principales conclusiones de este trabajo.

2. Revisión de Literatura

Existe una extensa literatura que relata la irrupción del Bitcoin en los mercados virtuales y el aumento de su uso en los últimos años; en la cual se enumeran las ventajas y posibles riesgos de este sistema; y se describen los desafíos legislativos y de regulación que conlleva el uso de este nuevo sistema. Un ejemplo de esta literatura es Turpin (2014) y el informe de 2014 de la Autoridad Bancaria Europea (en adelante EBA por su sigla en inglés)[2].

Asimismo, Rogojanu y Badea (2014) hacen una revisión del uso de monedas privadas alternativas a lo largo de la historia en países desarrollados y en vías de desarrollo. Luego, describen qué es el Bitcoin y cómo funciona. Posterior a esta descripción, enumeran las ventajas y desventajas de esta moneda virtual. Los autores consideran que la principal ventaja de su uso es la disminución de los costos de transacción, mientras que, entre las desventajas, destacan la volatilidad de la moneda y el anonimato con el que funciona el sistema. Los autores concluyen con algunas preguntas abiertas sobre el futuro del Bitcoin y su uso como una moneda alternativa a las monedas tradicionales.

Con respecto al impacto que podría tener el uso de la criptomoneda en los sistemas monetarios, Yermack (2013) analiza la evolución del precio del Bitcoin y su correlación con otras divisas y con un activo refugio como el oro. A partir de este análisis, el autor cuestiona el futuro uso del Bitcoin como moneda debido a la limitación de que no se puede utilizar para denominar préstamos ni créditos y, principalmente, a la gran volatilidad de su precio. Para el autor, la gran volatilidad que presenta la moneda virtual impide que sea usada como unidad de cuenta o reserva de valor, por lo que la define más bien como un instrumento de inversión especulativo.

Adicionalmente, Dwyer (2015) sostiene que el Bitcoin y las monedas digitales en general tienen el potencial de socavar la capacidad de un gobierno de generar ingresos a partir de la inflación. Este potencial adquiere gran importancia en economías que utilizan controles de cambio y de capital con el fin de mantener los dineros extranjeros y limitar los intercambios de moneda local por otras monedas por parte de los ciudadanos. Por este motivo, el autor destaca la posibilidad de evadir controles de capital como una de las principales características del Bitcoin.

Por el lado de la regulación y a partir del creciente uso de la moneda virtual en el mundo, Twomey (2013) argumenta que el principal defecto del sistema es el anonimato con el que funciona. El autor sostiene que el peligro del anonimato es que se facilitan actividades ilícitas como por ejemplo el lavado de dinero, la compra de drogas ilegales y el financiamiento de terrorismo. Por este motivo, en este trabajo se hace énfasis principalmente en la necesidad de regular el intercambio en Bitcoins a través de leyes. Finalmente, el autor propone medidas que se deberían tomar en el corto y largo plazo en materia de legislación, principalmente para EE.UU.

Así también, Tu y Meredith (2014) analizan los desafíos en regulación y legislación sobre las monedas virtuales en EE.UU., principalmente en los ámbitos de sistemas de pago, servicios financieros e inversiones. Asimismo, analizan los riesgos que conlleva este sistema, principalmente los relacionados con el anonimato y el lavado de dinero. Los autores proponen legislar considerando el uso global de la moneda virtual, como así también sus características únicas y distintivas.

[2] En el Anexo 1 se presenta un completo resumen del informe de la EBA de 2014

En esta misma línea están los trabajos de Lane (2013), Kirby (2014), De Filippi (2014) y Candelario (2015). Éste último además presenta un análisis de las leyes que han sido promulgadas en los países de América Latina para regular el uso de las monedas digitales.

Tsukerman (2015) presenta la historia del sistema y realiza un estudio sobre el estado de Bitcoin en EE.UU. El autor profundiza en el problema de la evasión de impuestos que conlleva el uso de la moneda virtual. Finalmente, realiza una revisión de las leyes que se podrían aplicar al sistema de Bitcoin en EE.UU. y presenta propuestas para el futuro.

Brito et al. (2015) presentan el desafío en regulación que genera el Bitcoin en las transacciones de instrumentos financieros, *securities* y derivados. Los autores realizan una descripción de las diferencias de este tipo de transacciones y proponen una regulación diferenciada en estos casos. En esta misma línea, está también la investigación de Harasic (2014).

Por su parte, Hendrickson et al. (2016) proponen un modelo con *matching* endógeno y preferencias de consumo aleatorias y encuentran múltiples equilibrios monetarios incluyendo uno en el que el Bitcoin coexiste con la moneda de curso oficial. Luego, los autores identifican las condiciones bajo las cuales la regulación de las transacciones puede desincentivar el uso de la moneda virtual. Finalmente, los autores demuestran que regular el uso de Bitcoin se hace más difícil si algunos usuarios prefieren la moneda digital para así evitar a los usuarios de moneda oficial en el proceso de *matching*.

Por otro lado, Kaplanov (2012) sostiene que un gobierno federal no tiene base legal para prohibir el uso de Bitcoin. El autor va más allá y en base a variados argumentos plantea que el gobierno debe abstenerse de aprobar cualquier ley o reglamento que limite el uso de la moneda virtual, ya que la ley no puede desincentivar el uso de nuevas tecnologías.

En esta misma línea, pero desde un punto de vista más teórico, Reyes (2016) analiza los fundamentos para una teoría endógena de regulación tecnológica descentralizada y propone los criterios para construir un marco regulatorio en este tipo de sistemas. El autor concluye advirtiendo los efectos negativos de desincentivar la innovación.

Profundizando en el tema de la innovación, Dodgson et al. (2015) destacan la importancia del dinero digital como una innovación transformacional y las consecuencias y oportunidades que esto conlleva para la academia de *management*. En el uso del dinero digital, los autores destacan tres elementos que justifican la innovación del modelo de negocios: la búsqueda de ganancias de eficiencia mediante la reducción de la fricción causada en las transacciones financieras tradicionales, nuevas formas de interacción con los clientes y la creación de nuevos negocios basados en los datos obtenidos del comportamiento transaccional (datos sobre patrones de compra, transacciones y flujo de dinero). En esta misma línea, se sostiene que las mejoras en la eficiencia operativa son un factor clave al considerar cambios en el modelo de negocios en las empresas ya establecidas, particularmente en torno a la reducción de costos de transacción y de contabilidad. Por todo lo anterior, los académicos de *management* tendrían el desafío de explorar y explicar los beneficios de ser un incumbente o entrante ante esta revolución financiera. Particularmente en el Bitcoin, los autores destacan la seguridad en las transacciones y los menores costos de éstas, y advierten sobre los riesgos que conlleva su volatilidad, la ausencia de supervisión y protección del consumidor, la facilidad de realizar lavado de dinero y la irreversibilidad de las

transacciones. Los autores sostienen que la tecnología detrás de Bitcoin, el *blockchain*, tienen un gran potencial para el desarrollo de los mercados financieros. Además, argumentan que la gran popularidad del Bitcoin surgió a partir de la posibilidad que entrega a los trabajadores extranjeros de enviar dinero a sus países de origen con mayor facilidad y a un menor costo. A partir de esto último, precisan que el sistema trae consigo una innovación inclusiva, ya que propone soluciones para trabajadores de menores ingresos y provenientes de países en desarrollo y, además, facilita el emprendimiento en estos países. Luego, los autores discuten sobre la transición desde la confianza en un intermediario financiero hacia un sistema en que se confía en la reputación de agentes anónimos y en un chequeo de la autenticidad realizado por parte de la comunidad de usuarios, denominados mineros[3].

Por otro lado, la literatura que analiza la tecnología *blockchain* de forma rigurosa es bastante reducida. Por ejemplo, Lee Kuo Chuen (2015) realiza un completo estudio sobre las criptomonedas, particularmente sobre el Bitcoin, pero el autor sólo dedica una breve sección a la descripción de la tecnología *blockchain* y el trabajo de minería.

Nakamoto (2008), entidad creadora del Bitcoin, explica cómo el sistema *blockchain* es capaz de resolver el problema del doble pago simultáneo sin necesidad de intermediarios financieros. El autor presenta las principales características de esta tecnología que permiten realizar transacciones electrónicas sin depender de la confianza en una tercera parte.

Becker et al. (2013) realizan un completo análisis del concepto de prueba de trabajo (*proof-of-work*)[4] y su aplicación a un sistema distribuido de transacciones sin un control centralizado como es Bitcoin. Particularmente, se enfocan en la capacidad del sistema de evitar el doble gasto y de administrar la escasez, dos propiedades esenciales para cualquier moneda electrónica. Previo a su análisis, los autores realizan una revisión de las principales características que hacen de *blockchain* un sistema seguro y difícil de vulnerar.

Möser et al. (2013) estudian los riesgos del carácter pseudoanónimo de Bitcoin, principalmente enfocados en que el sistema permitiría el lavado de dinero y otras actividades ilícitas. Para esto, en primer lugar, realizan una descripción del sistema Bitcoin y la tecnología *blockchain*, enfocados principalmente en las transacciones realizadas con el sistema.

Así también, Böhme et al. (2015) realizan un completo estudio sobre cómo se realizan las transacciones en el sistema de Bitcoin y el rol de la tecnología *blockchain* en este tipo de operaciones. Luego, los autores realizan un análisis sobre los riesgos del uso del Bitcoin, los desafíos regulatorios y los potenciales efectos en la conducción de la política monetaria de los países.

Finalmente, Malinova y Park (2016) analizan la irrupción de la tecnología *blockchain* y plantean que la implementación de esta tecnología en los mercados financieros ofrece a los inversores nuevas opciones para gestionar el grado de transparencia de sus participaciones y de las intenciones de sus operaciones. Los autores presentan un modelo teórico de transacciones entre dos partes con

[3] Los mineros son ordenadores/chips dedicados a aportar poder computacional a la red de Bitcoin para verificar las transacciones que se llevan a cabo. Cada vez que un minero completa un bloque, recibe una recompensa en forma de Bitcoins. Además, en algunos casos, reciben una recompensa a partir de pequeñas tarifas de transacción. A lo largo del trabajo, se explica en detalle esta labor.

[4] Este concepto se explica en detalle en la sección 5.

intermediarios financieros. A partir de este modelo, analizan cómo el diseño de implementación de ciertas características críticas afecta el comportamiento de los inversores, los costos de negociación y el bienestar de los inversionistas. Los autores encuentran que, a pesar del riesgo de *front-running*, un entorno más transparente genera un mayor bienestar para los inversores. Además, ante la falta de transparencia total, y para niveles bajos de liquidez en el mercado intermediado, el bienestar es mayor si se requiere que los inversores concentren sus participaciones bajo identificadores únicos.

Como se puede observar, a diferencia de la gran cantidad de trabajos que discuten sobre los desafíos regulatorios que conlleva el uso de Bitcoin, la literatura que ha estudiado *blockchain* de forma rigurosa no es muy extensa. Por ende, este trabajo abordará exhaustivamente este punto. Pero antes, en la siguiente sección, se explica en detalle el concepto de Bitcoin y su irrupción en el mercado de comercio electrónico.

3. Bitcoin y su irrupción en el mercado de comercio electrónico

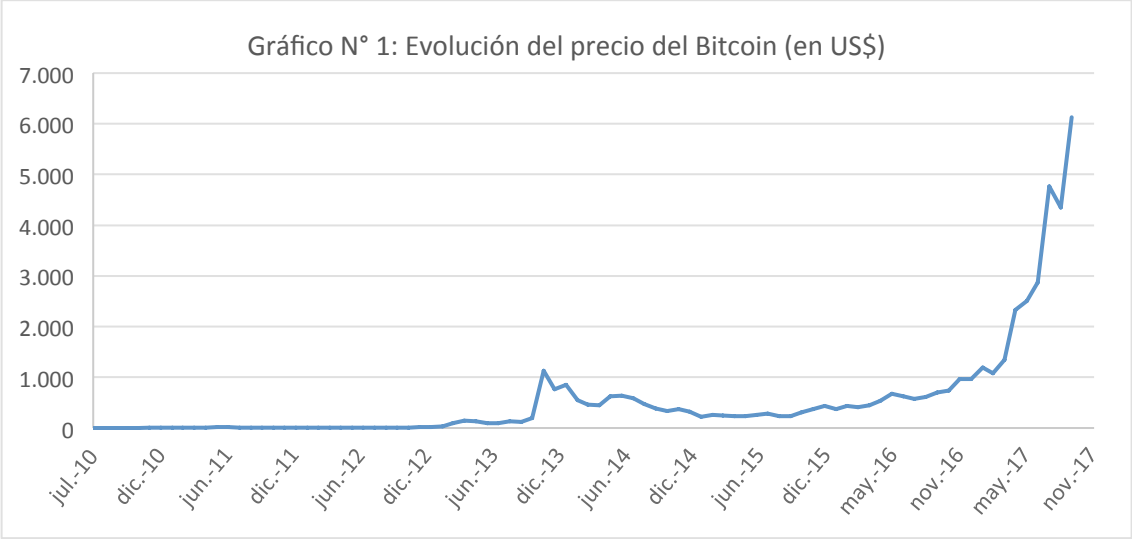
Bitcoin es una de las primeras implementaciones de un concepto denominado criptodivisa o criptomoneda, que consiste en una moneda virtual generada de forma distribuida, por un único organismo, sin control de parte de algún gobierno y de un carácter anónimo. Esta moneda permite efectuar transacciones de forma segura y sin la necesidad de un intermediario financiero ni de pago de comisiones[5]. Al contrario de las monedas convencionales convertibles, el Bitcoin no está respaldado ni regulado por ningún ente emisor, como por ejemplo un gobierno o un banco central. Por esta razón, se define como una moneda críptica, cifrada y anónima.

Actualmente, la totalidad de las divisas usadas en la economía mundial son dinero fiduciario, es decir, dinero emitido por bancos centrales, sin respaldo de metal precioso y basado en la confianza de los actores del mercado. Por su parte, Bitcoin usa un sistema de prueba de trabajo *(proof-of-work system*). Este consiste en poner un cierto trabajo a quienes soliciten Bitcoins (el llamado trabajo de minería, que consiste en poner a disposición del sistema equipos computacionales que operen como servidores), para que finalmente puedan obtenerlos a partir de un algoritmo matemático. Para evitar que la oferta de esta moneda virtual aumente de forma desproporcionada, a través del algoritmo mencionado, se ajusta la dificultad o duración de los trabajos, evitando así la inflación. De esta forma, el valor de un Bitcoin se acerca a su costo marginal de producción. Por lo anterior, la moneda no está sujeta a shocks de oferta y su escasez no es natural. Esta situación contrasta con el dinero fiduciario, donde el costo de producir el dinero no tiene relación alguna con su valor, de manera tal que una gestión descuidada o politizada de la emisión de dinero fiduciario aumente la posibilidad de una alta inflación.

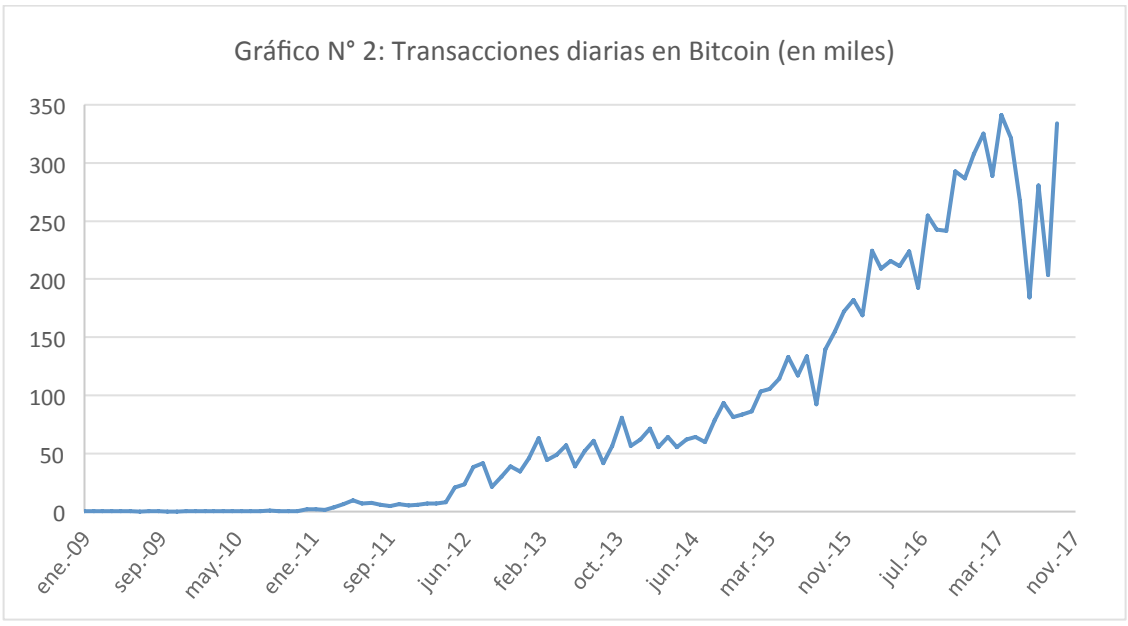
Su creación se remonta a 2008, año en que el concepto de Bitcoin fue desarrollado por un grupo de personas bajo el seudónimo de *Satoshi Nakamoto*. En 2009, éste comienza a operar formalmente y en 2010 este grupo abandonó el proyecto sin revelar su identidad y generando gran sorpresa.

[5] En un principio la red era casi gratuita pero actualmente existe la opción de pagar por priorizar o acelerar la transacción. Este pago está en torno a los 3-4 dólares.

Actualmente, el precio del Bitcoin está en torno a los US$6.100 y se realizan alrededor de 300 mil transacciones diarias. En los gráficos N° 1 y 2 se muestra la evolución del precio de la criptomoneda en el tiempo y el aumento de las transacciones diarias en Bitcoin, respectivamente.



Fuente: Elaboración propia a partir de datos de CoinDesk



Fuente: Elaboración propia a partir de datos de blockchain.info

Se puede observar un notorio aumento de precio en los últimos meses. Mientras gran parte de los bancos centrales advierten sobre el peligro de estar ante una burbuja a punto de estallar, algunos analistas sostienen que este aumento del precio estaría bien fundamentado y causado principalmente por:

1. La percepción de seguridad. Los recientes ataques cibernéticos como *Wannacry* han llevado a un aumento en la demanda de Bitcoin y, por ende, a un alza de su precio, debido a la percepción de estar protegidos de este tipo de ataques cuando se utiliza la moneda virtual.
2. La legalización de su uso en Japón, y una posible futura legalización en Rusia.
3. El aumento de la demanda en China para intercambio doméstico y para evitar el control de capitales.
4. El proceso de desmonetización de algunos países en el mundo como India, Pakistán, España y Venezuela.
5. La incertidumbre con respecto a la administración de Trump.

Con el paso de los años, las alternativas para transar con este sistema han aumentado. Se presentan así distintas opciones que cambian unos beneficios por otros. Las aplicaciones independientes otorgan anonimato y mayor seguridad, pero sin los cuidados necesarios, el usuario puede perder su clave privada o su respaldo y, con éstos, sus Bitcoins. Por otro lado, las carteras en línea eliminan el problema de las claves y respaldos, pero sacrifican el anonimato y agregan factores externos de riesgo como por ejemplo *hacks* a la plataforma e indisponibilidad de fondos, entre otros. En otras palabras, los usuarios enfrentan un *trade-off* entre anonimato y seguridad vs respaldo.

Algunos autores prefieren clasificar a Bitcoin como una red basada en seudónimos en lugar de una red anónima. El uso de seudónimos, al contrario del anonimato, ofrece la posibilidad de generar una reputación y confianza entre los usuarios. Para facilitar el análisis de todos los movimientos, varios sitios web proporcionan información actualizada de todas las transacciones, incluyendo variables agregadas como el número de Bitcoins en circulación, número de transacciones por hora y tarifas de transacción en cada instante. Como el núcleo del protocolo Bitcoin no cifra ningún tipo de información, todas las transacciones son públicas y cualquier observador externo puede analizar en todo momento su contenido, el origen y el destino de todos los mensajes. Esta característica contrasta con el modelo bancario tradicional que oculta las transacciones del escrutinio público.

A continuación, para lograr un mayor entendimiento del sistema, se presenta una breve descripción de cómo funciona el sistema tradicional de transferencias bancarias para luego, adentrarse en el estudio de esta nueva tecnología llamada *blockchain*.

4. Sistema tradicional de transferencias bancarias

A continuación, se presenta una explicación simplificada de cómo funcionan los sistemas de depósitos, pagos y transferencias en el sistema bancario tradicional.

Primero que todo, resulta útil definir los depósitos bancarios como pasivos. De esta forma, cuando una persona deposita dinero electrónicamente en un banco, realmente no tiene un depósito. El dinero no está físicamente en un lugar a nombre de la persona. En cambio, la transacción figura como un préstamo que realiza la persona al banco, por lo tanto, se convierte en un pasivo para el banco. Es por eso que se dice que la cuenta está en crédito, ya que se ha extendido un crédito al

banco. Del mismo modo, si una persona está sobregirada y debe dinero al banco, éste se convierte en su responsabilidad y un activo para el banco. Para entender lo que está pasando cuando el dinero se mueve, es importante darse cuenta de que cada saldo en la cuenta se puede ver de estas dos maneras, es decir, desde la posición de la persona y desde la posición del banco.

Cuando una persona deposita dinero a otra y ambas utilizan cuentas del mismo banco para la transacción, el proceso es bastante simple. Si una persona debe depositar U$100 a otra, debe avisar al banco lo que desea hacer y el banco debita los fondos de su cuenta y genera un crédito en la cuenta de quien recibe el depósito. Este proceso se hace electrónicamente en el sistema central del banco y es bastante simple ya que no entra ni sale dinero del banco. Sólo se realiza una actualización de su sistema de contabilidad. Ahora, el banco le debe U$100 menos a quien transfiere el dinero y U$100 más a quien recibe el dinero en la transferencia. Todo se equilibra y se hace dentro del banco, es decir, se puede afirmar que la transacción se "liquidó" en los libros del banco. En este caso el banco actúa como intermediario financiero, es decir, como tercera parte de confianza.

En el caso en que una persona debe depositar dinero a otra y ambas utilizan cuentas de distintos bancos, el proceso se hace más complejo. Cuando una persona decide transferir dinero a otra persona en una cuenta de otro banco, además de las cuentas de estas dos personas, se utilizan las cuentas bancarias que un banco tiene en el otro.

Así, en términos simplificados, el proceso es el siguiente:

1. Banco de la persona que transfiere (banco 1) reduce saldo de la cuenta de la persona que transfiere en U$100.
2. Banco de la persona que transfiere (banco 1) añade U$100 a la cuenta del banco de la persona que recibe el dinero (en cuenta que banco 2 tiene en banco 1).
3. Banco de la persona que transfiere (banco 1) avisa a banco de la persona que recibe el dinero (banco 2) que ha aumentado el saldo de la cuenta del banco de la persona que recibe el dinero (cuenta que banco 2 tiene en banco 1) y solicita aumentar el saldo de la cuenta de quien recibe el depósito en su banco.
4. Banco de la persona que recibe el dinero (banco 2) recibe el mensaje y al confirmar un aumento del saldo en la cuenta que poseen en el banco de la persona que transfiere (cuenta que banco 2 tiene en banco 1), aumenta el saldo de la cuenta de la persona que recibe el dinero.

De este modo, la persona que transfiere dinero tiene U$100 dólares menos en la cuenta de su banco y la persona que recibe el dinero, tiene U$100 dólares más en la cuenta de su banco.

Antes de la transferencia, el banco del depositante le debía U$100 al depositante y luego de la transferencia, le debe U$100 al banco de la persona que recibe el depósito. Antes de la transferencia, el banco de la persona que recibe el dinero no tenía pasivos ni activos y luego de la transferencia, le debe U$100 a la persona que recibió el depósito y el banco del depositante le debe U$100.

Este modelo de procesamiento de pagos se conoce como corresponsalía bancaria y en él destaca que la existencia de un acuerdo bancario correspondiente permite facilitar los pagos entre sus respectivos clientes.

Este proceso simplificado funciona bastante bien, pero tiene algunos problemas importantes:

1. Sólo funciona si los dos bancos tienen una relación directa entre sí, es decir, si uno posee cuenta en el otro. Si no es así, no se pueden realizar transferencias de forma tan directa y se necesita utilizar las cuentas de un tercer o hasta cuarto banco hasta completar el camino entre la persona que transfiere el dinero y quien lo recibe. Esto aumenta el costo y la complejidad de la transacción. Así, la interconexión inherente a este modelo es un problema muy real.
2. Es arriesgado para el banco de quien recibe el dinero. Luego de una transacción, su exposición al banco de quien realiza el depósito aumenta. El banco de quien recibe el dinero tendría un gran problema si el banco de quien realiza la transferencia quebrara. Para solucionar este problema, el banco de la persona que transfiere, en vez de aumentar el saldo de la cuenta del banco de la persona que recibe el dinero, podría solicitar al banco de quien recibe el dinero que disminuya el saldo de la cuenta que el banco de quien transfiere tiene en el banco de la persona que recibe el dinero. De esta manera, los grandes saldos interbancarios podrían no acumularse. Sin embargo, hay otros problemas con este sistema simplificado.

Para este proceso, se podría utilizar la red SWIFT que permite a los bancos intercambiar mensajes electrónicos entre sí de forma segura. Esta red se utiliza para administrar el flujo de información entre bancos y asegurarse de que estas transferencias se producen de forma rápida, confiable y a un costo razonable. Uno de los tipos de mensajes admitidos por la red SWIFT es MT103. El mensaje MT103 permite a un banco instruir a otro banco para que acredite la cuenta de uno de sus clientes, debitando la cuenta de la entidad emisora con el banco receptor para equilibrar todo. Por lo tanto, el efecto de un SWIFT MT103 es "enviar" dinero entre los dos bancos, pero es importante notar lo que está sucediendo. El mensaje de SWIFT es simplemente la instrucción. El movimiento de los fondos se realiza mediante débito y acreditación de varias cuentas en cada institución y se basa en que los bancos mantengan cuentas entre sí (ya sea directamente o a través de bancos intermediarios).

A continuación, se abordan otras dificultades que surgen en este proceso: costos de transacción, liquidez y riesgo de contraparte.

En primer lugar, se debe reconocer que SWIFT no es barato. Si un banco tuviera que enviar un mensaje SWIFT a otro cada vez que quisiera pagar un monto pequeño a alguien que recibe una transferencia, pronto notaría un fuerte aumento de sus costos. Además, existe una fuerte restricción de liquidez: Imagine todo el dinero que el banco de la persona que transfiere tendría que tener depositado en todos sus bancos corresponsales todos los días si el sistema descrito anteriormente se utilizara en la práctica. Tendrían que mantener saldos considerables en todos los otros bancos sólo en caso de que uno de sus clientes quisiera enviar dinero a una persona con cuenta en otro banco. Se trata de dinero en efectivo que podría ser invertido, prestado o puesto a trabajar de otra manera.

Se debe notar que tan probable como que una persona con cuenta en el banco A transfiera dinero a una persona con cuenta en el banco B, es que una persona con cuenta en el banco B transfiera dinero a una persona con cuenta en el banco A.

Lo que se hace entonces, es que se realiza un registro de todas las transferencias que se realizan durante el día y solo se liquida el saldo final. Lo anterior consiste en un sistema diferido de liquidación neta. En este sistema, los mensajes no se intercambian a través de SWIFT. En su lugar, los mensajes (o archivos) se envían a un sistema central de compensación, que realiza un seguimiento de todos los pagos y luego calcula la cantidad neta debida por cada banco entre sí. Esto reduce drásticamente los costos de transacción y las demandas de liquidez.

Este enfoque introduce otro problema importante: se pierde la finalidad de la liquidación. Es posible emitir una instrucción de pago por la mañana, pero el banco receptor no recibe los fondos (netos) hasta el final del día. Por lo tanto, el banco receptor tendría que esperar hasta que reciban la liquidación (neta). Lo anterior, debido a que el banco emisor podría reversar alguna transacción, por lo que sería imprudente liberar fondos al cliente receptor antes de ese momento. Esto introduce un retraso en las trasferencias.

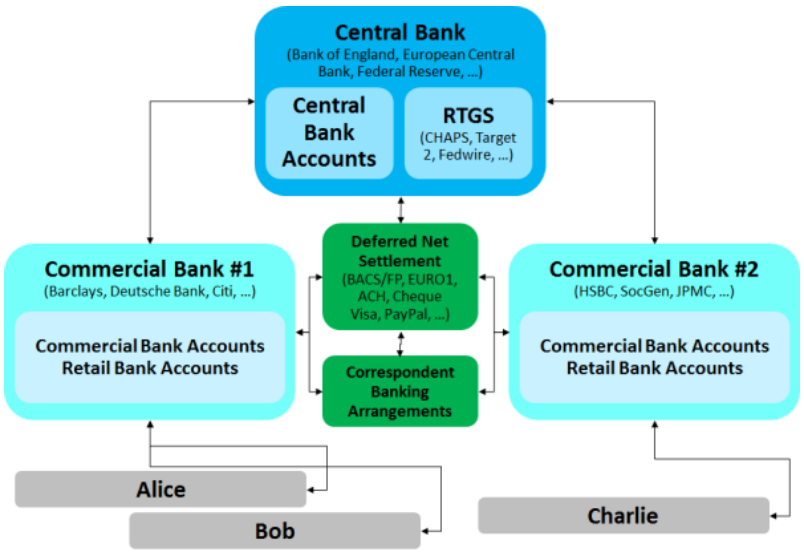
Una alternativa sería asumir el riesgo, pero revertir la transacción en caso de algún problema. En este caso, la transferencia no podría en ningún caso ser considerada definitiva, por lo que el beneficiario no podría confiar en los fondos hasta transcurrido todo el día.

Para alcanzar una liquidación pronta de las transacciones y riesgo cero de la contraparte, se debe incorporar otro elemento o parte al sistema. Ninguno de los enfoques que se ha esbozado hasta el momento es realmente aceptable para situaciones en las que es necesario estar absolutamente seguro de que el pago se realizará rápidamente y no se puede revertir. Se requiere cierta garantía, sobre todo cuando se trata de grande sumas de dinero.

Lo que se necesita es un sistema que funcione como una transacción entre cuentas del mismo banco, pero que funcione cuando más de un banco está involucrado. El sistema bancario multilateral esbozado anteriormente funciona, pero se aumentan los riesgos cuando las cantidades involucradas se hacen grandes y cuando existe la posibilidad de que uno u otro de ellos pueda ir a la quiebra.

A partir de lo anterior, se incorpora la figura del banco central. Al incorporarla, los bancos de un país pueden mantener cuentas con el banco central, por lo que pueden transferir dinero entre sí simplemente instruyendo al banco central a debitar una cuenta y/o acreditar otra. Este sistema permite movimientos de fondos en tiempo real entre las cuentas mantenidas por los bancos en sus respectivos bancos centrales. Esto consiste en un sistema de Liquidación Bruta en Tiempo Real: Tiempo real porque sucede inmediatamente; bruto porque no se requiere compensación (de lo contrario no podría ser instantánea); y de liquidación porque en principio tiene carácter definitivo y sin reversiones. En la Figura N° 1 se presenta el esquema completo de transferencias bancarias en sistema tradicional.

Figura N° 1: Esquema de transferencias bancarias en sistema tradicional



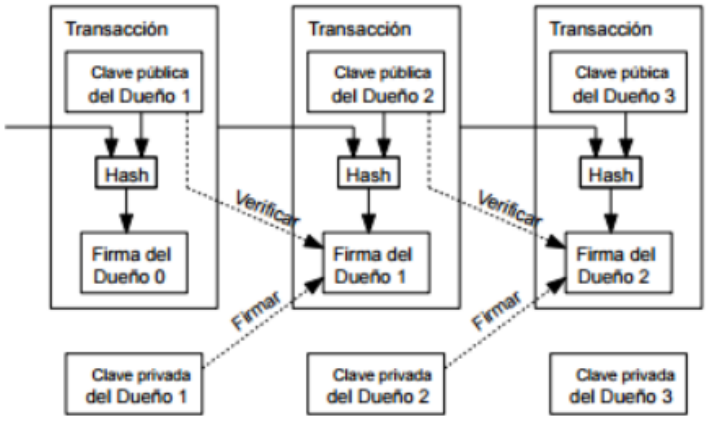
Fuente: https://gendal.me/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-banking-system/

4.1 Autentificación de una transacción en el sistema bancario tradicional

Primero que todo, se define una moneda electrónica como una cadena de firmas digitales. En términos simples, el dueño de una moneda electrónica puede transferir su dinero a otra persona firmando digitalmente (con su clave privada) un *hash*[6] de la transacción previa (es decir, se realiza la orden de dar salida a dinero que previamente había entrado), indicando la cuenta de destino del próximo dueño, y agregando la firma y la cuenta de destino al final de la moneda. Quien recibe el dinero puede observar la cuenta de origen y verificar el propietario inmediatamente anterior. En la Figura N° 2 se ilustra el proceso de autentificación de una transacción en el sistema bancario tradicional. En este caso, la clave pública consiste en la información sobre la cuenta bancaria de las personas y la firma consiste en la orden de realizar la transacción.

[6] En el Anexo 2 se presenta una descripción del concepto *hash.*

Figura N° 2: Proceso de autentificación de una transacción en el sistema bancario tradicional



Fuente: Traducción de figura original de Nakamoto (2008)

Un problema importante de este sistema es que quien recibe la moneda electrónica no puede verificar si alguno de los dueños previos hizo un doble gasto de la moneda. Es decir, el dueño de una moneda podría indicar el depósito de una misma moneda en dos cuentas de destino diferentes, y quienes la reciben, no pueden verificar si esto está ocurriendo o no.

La solución común a este problema es introducir un intermediario financiero, que revise si la moneda utilizada en una transacción tiene doble gasto o no. Después de cada transacción, la moneda debe ser devuelta al intermediario para generar una nueva moneda, de modo que solo las monedas generadas directamente por este intermediario, son las que se asume (confía) que no tienen doble gasto.

Así, el destino del sistema monetario entero, depende de intermediarios que generen confianza entre las partes, y todas las transacciones son supervisadas por ellos.

Este sistema funciona suficientemente bien para la mayoría de las transacciones, sin embargo, padece de las debilidades inherentes de un modelo basado en confianza. Las transacciones completamente irreversibles no son realmente posibles, debido a que las instituciones financieras que operan como intermediarios no pueden evitar la mediación en disputas.

Adicionalmente, el costo de la intermediación incrementa los costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de realizar pequeñas transacciones casuales. Esta limitación se suma a la imposibilidad de hacer pagos irreversibles por servicios que también lo son.

Con la posibilidad de revertir una transferencia, la necesidad de confianza aumenta. Los comerciantes deben tener precaución al elegir a sus clientes y solicitarles más información de la que se necesitaría en un sistema de transacciones irreversibles.

Estas limitaciones e incertidumbre en la liquidación final de los pagos pueden ser evitadas si la persona utiliza dinero físico, pero hasta antes de la irrupción de Bitcoin y la tecnología *blockchain*, no existía un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable.

5. Tecnología *blockchain* aplicada a sistema Bitcoin

A raíz de los inconvenientes que pueden surgir al utilizar el sistema tradicional, es posible delinear las características que debería tener un sistema para que no presente las debilidades antes señaladas[7]. Así, se requiere diseñar un sistema en el que quien recibe la moneda pueda saber que el dueño previo (anterior) no firmó ninguna transacción anterior. Para esto, la transacción más reciente es la que cuenta. La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las transacciones existentes. En el modelo tradicional, el intermediario financiero es el que está al tanto de todas las transacciones y es quien revisa cuáles llegan primero.

Para hacer posible esta supervisión sin una tercera parte confiable, las transacciones deben ser anunciadas públicamente, por lo que se requiere de un sistema de participantes que estén de acuerdo en una historia única del orden en que estas transacciones fueron realizadas. Quien recibe la moneda necesita saber que, en el momento de cada transacción, la mayoría de los participantes estuvieron de acuerdo en cuál fue la primera transacción que se recibió.

Así, se origina un sistema de pagos electrónicos que está basado en pruebas criptográficas en vez de confianza, permitiendo a las dos partes interesadas realizar transacciones directamente sin la necesidad de una tercera parte confiable. De esta forma, transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, del mismo modo que mecanismos rutinarios de depósito de garantía podrían ser fácilmente implementados para proteger a los compradores. El sistema que posee estas características es conocido como *blockchain* o cadena de bloques.

Este sistema consiste en una solución al problema del doble gasto utilizando un servidor de marcas de tiempo usuario-a-usuario distribuido[8] para generar una prueba computacional del orden cronológico de las transacciones. El sistema es seguro mientras los participantes "honestos" controlen colectivamente más poder de procesamiento computacional que cualquier grupo de participantes que quieran vulnerar el sistema.

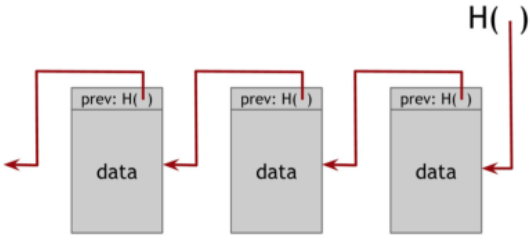
Una cadena de bloques, o *blockchain*, también conocida como libro de contabilidad distribuido (*distributed ledger*), es una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de la información y la verificación de que ésta no ha sido cambiada. Los bloques de información se enlazan mediante apuntadores *hash* que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al bloque génesis. Esto se ilustra en la Figura N° 3. La cadena de bloques es almacenada por todos aquellos nodos[9] de la red que se mantienen en sincronía con ésta.

[7] El análisis de las innovaciones que han surgido dentro del marco del sistema bancario tradicional como respuesta a la irrupción de *blockchain* queda pendiente para una futura investigación. Entre éstas, podemos encontrar principalmente dos: la primera, el surgimiento de las empresas *fintech*, que, a través del uso de las nuevas tecnologías, buscan realizar el trabajo de intermediación y proveer servicios financieros a los clientes a menor costo. La segunda, es la creación de una nueva regulación europea en materia de pagos que implica cambios fundamentales en la industria al dar acceso a terceros a la infraestructura de los bancos, denominada PSD2.

[8] En el Anexo 3 se presenta una explicación del concepto *distribuido*.

[9] Un nodo es un ordenador/chip conectado a la red Bitcoin que utiliza un software que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques. Cada vez que un bloque se confirma y se añade a la cadena, esto se comunica a todos los nodos y el bloque se añade a la copia que cada nodo almacena.

Figura N° 3: Enlace de bloques de información mediante *hash*

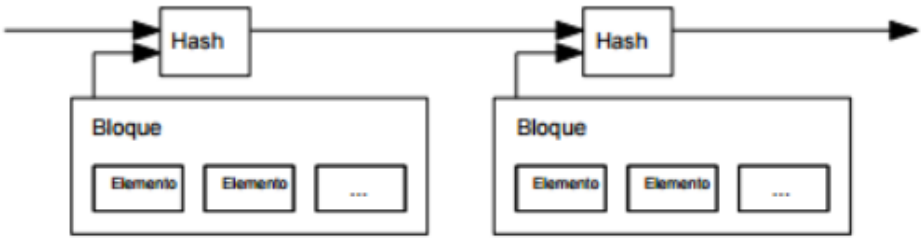


A continuación, de presentan los principales elementos y características de la tecnología *blockchain* aplicada al sistema de la criptomoneda Bitcoin.

5.1 Servidor de marcas de tiempo

El sistema cuenta con un servidor de marcas de tiempo. Un servidor de marcas de tiempo funciona al realizar el *hash* de un bloque[10] de datos a ser fechados y publicándolo ampliamente, tal y como se haría en un periódico. La marca de tiempo prueba que el dato, obviamente, debió de haber existido en ese momento para poder incluirse dentro del *hash*. Cada marca de tiempo incluye en su *hash* la marca de tiempo previa, formando una cadena, de modo que cada marca de tiempo adicional refuerza las anteriores a una dada.

Figura N° 4: Marca de tiempo y *hash*



Fuente: Traducción de figura original de Nakamoto (2008)

5.2 Prueba de trabajo (*proof of work*)

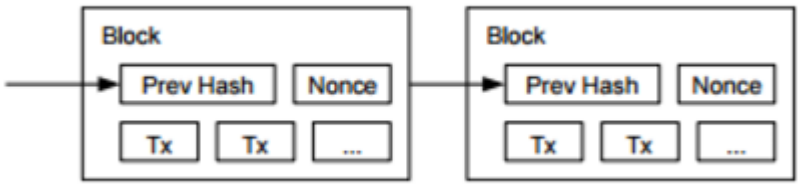
Para implementar un servidor de marcas de tiempo siguiendo un esquema usuario-a-usuario, se requiere utilizar un sistema de prueba de trabajo, en vez de usar una publicación en un periódico. La prueba de trabajo implica la exploración de un valor, tal que, al calcular un *hash*, éste empiece con un número determinado de *bits* con valor cero. El trabajo promedio requerido será exponencial al número de *bits* requeridos con valor cero pero que pueda ser verificado ejecutando un solo *hash*.

Una de las mayores innovaciones que tiene el protocolo Bitcoin es que cada unidad no es un archivo como tal que se envía como si fuese una película o canción. En realidad, lo que se produce es un registro del cambio de propiedad de una cantidad determinada de Bitcoins en la cadena de bloques.

[10] En el Anexo 4 se presenta una descripción de qué es un bloque.

Para esta red de marcas de tiempo se implementa la prueba de trabajo incrementando el valor de un campo *nonce*[11], perteneciente al bloque, hasta que se encuentre un valor que dé el número requerido de *bits* con valor cero para el *hash* del mismo. Una vez que el esfuerzo computacional se ha realizado para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo. A medida que más bloques son encadenados después de uno dado, el trabajo para cambiar un bloque incluiría rehacer todos los bloques después de éste.

Figura N° 5: Inclusión de *nonce* en prueba de trabajo



Fuente: Nakamoto (2008)

La prueba de trabajo también resuelve el problema de determinar cómo representar la decisión por mayoría. Si la mayoría se basara en un voto por dirección IP, podría ser alterada por alguien capaz de asignar muchas IPs. La prueba de trabajo equivale esencialmente a "una-CPU-un-voto". La decisión de la mayoría es representada por la cadena más larga, la cual posee la prueba de trabajo con mayor esfuerzo invertido[12]. Si la mayoría del poder de CPU está controlado por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás cualquier otra cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba de trabajo del bloque y de todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos.

5.3 Cómo funciona la red

Los pasos que ejecuta la red son los siguientes:

1. Las nuevas transacciones son emitidas a todos los nodos.
2. Cada nodo recolecta nuevas transacciones en un bloque.
3. Cada nodo trabaja en encontrar una prueba de trabajo difícil para su bloque.
4. Cuando un nodo encuentra una prueba de trabajo, emite el bloque a todos los nodos.
5. Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas, es decir, si sólo se transfieren monedas que aún no han sido gastadas (transferidas por su dueño).

[11] En criptografía, el termino *nonce* es usado para referirse a un valor que solamente puede ser usado una vez. Este número único o *nonce*, es un número aleatorio emitido por los mineros a través de la prueba de trabajo (*proof of work*) que sirve para autenticar el bloque actual y evitar que la información sea reutilizada o cambiada sin realizar todo el trabajo nuevamente.

[12] Para compensar el incremento de la capacidad computacional en el tiempo, la dificultad de la prueba de trabajo es determinada por una media móvil dirigida por un número promedio de bloques a la hora. Si estos se generan muy rápido, la dificultad se incrementa.

6. Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el *hash* del bloque aceptado como *hash* previo.

Los nodos siempre consideran la cadena más larga como la correcta y verdadera, para luego empezar a trabajar en extenderla. Si dos nodos emiten versiones diferentes del próximo bloque simultáneamente, algunos nodos puede que reciban uno o el otro primero. En ese caso, trabajan en el primero que reciban, pero guardan la otra rama en caso de que esta se vuelva más larga. El empate se rompe cuando se encuentra la próxima prueba de trabajo y una rama se vuelve más larga; los nodos que estaban trabajando en la otra rama posteriormente se cambian a la que ahora es más larga.

Las emisiones de nuevas transacciones no necesariamente necesitan llegar a todos los nodos. En el momento que éstas llegan a muchos nodos, acabaran entrando en un bloque antes de que pase mucho tiempo. La emisión de los bloques también es tolerante a la pérdida de mensajes. Si un nodo no recibe un bloque, lo pedirá cuando reciba el próximo bloque y se dé cuenta que perdió uno.

5.4 Incentivos a supervisar el sistema

Por convención, la primera transacción en un bloque es una transacción especial que da origen a una nueva moneda otorgada al nodo creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red y proporciona una forma de distribuir inicialmente las monedas en circulación, ya que no existe una autoridad central que las emita.

La adición constante de una cierta cantidad (decreciente) de monedas nuevas es análoga a los mineros de oro que gastan recursos para agregar oro a la circulación[13]. En este caso, los recursos consisten en el tiempo utilizado en el computador y la electricidad requerida para su funcionamiento.

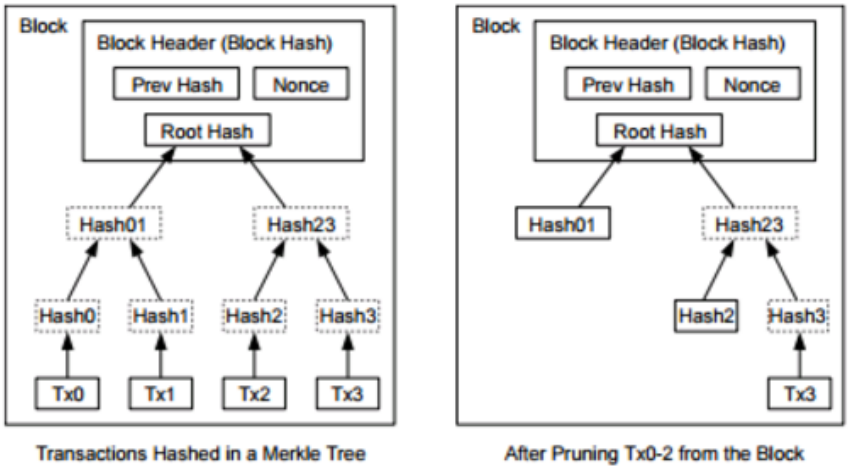
El incentivo también podría ser financiado con tarifas de transacción. Si el valor de salida de una transacción es menor que su valor de entrada, la diferencia es la tarifa de transacción que se agrega al valor de incentivo del bloque que contiene la transacción. Una vez que un número predeterminado de monedas ha entrado en circulación, el incentivo puede pasar a ser solamente la tarifa de transacción y ser totalmente libre de inflación. Este incentivo ayuda a incentivar a los nodos a mantenerse honestos. Si un atacante codicioso es capaz de reunir más potencia de CPU que todos los nodos honestos, tendría que elegir entre usarlo para defraudar a los usuarios mediante el robo de sus pagos o usarlo para generar nuevas monedas. Debería encontrar más rentable jugar siguiendo las reglas, ya que éstas lo favorecerían otorgándole más monedas nuevas que a la suma de todos los demás nodos, que socavar el sistema y la validez de su propia riqueza.

[13] Este tema se abordará con mayor detalle en la sección 6.2.

5.5 Recuperación de espacio en disco

Una vez que la última transacción está enterrada bajo suficientes bloques, las transacciones ya realizadas pueden ser descartadas para ahorrar espacio en disco[14]. Para facilitar esto sin romper el *hash* del bloque, las transacciones se comprueban en un árbol de Merkle[15], incluyendo solo la raíz en el *hash* del bloque. Los bloques viejos pueden entonces ser compactados cortando las ramas del árbol. De esta forma, los *hashes* interiores no necesitan ser almacenados. Esto es representado en la Figura N° 6.

Figura N° 6: Estructura e información contenida en un bloque de la cadena de bloques



Fuente: Nakamoto (2008)

5.6 Verificación de pagos simplificada

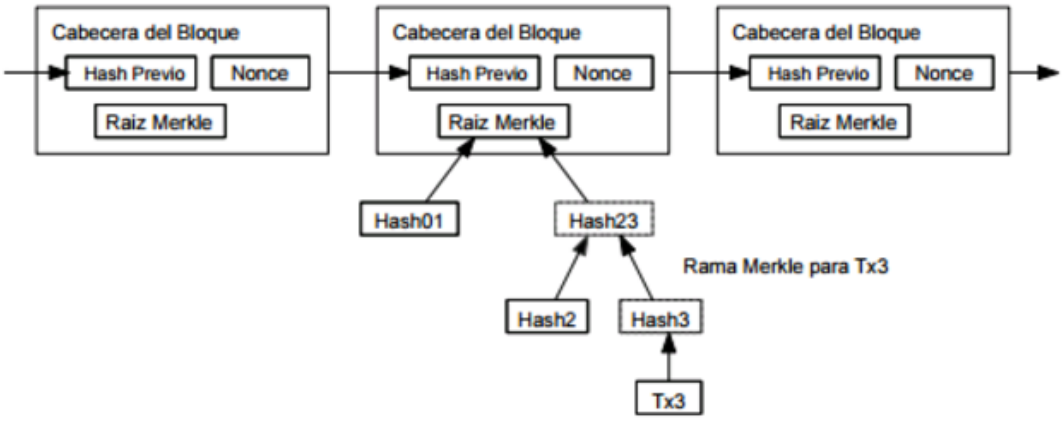
Es posible verificar pagos sin ejecutar un nodo de red completo. Un usuario solo necesita mantener una copia de los encabezados de los bloques de la cadena más larga de la prueba de trabajo, la que puede obtener haciendo una búsqueda en los nodos de la red hasta que esté convencido de tener la cadena más larga, y obtener la rama del *árbol de Merkle*, que enlaza la transacción con el bloque en que ha sido fechado.

Aunque no puede verificar la transacción por sí mismo, al enlazarla a algún lugar de la cadena, puede ver que algún nodo de la red la ha aceptado, de modo que los bloques añadidos después confirmarían aún más esta aceptación por parte de la red.

[14] Un encabezado de bloque sin transacciones sería de unos 80 *bytes*. Si suponemos que los bloques se generan cada 10 minutos, 80 *bytes* x 6 x 24 x 365 = 4.2MB por año. Los sistemas informáticos tradicionales cuentan con 2 GB de RAM a partir de 2008, y la Ley de Moore predice un crecimiento actual de 1,2 GB al año. Por lo tanto, el almacenamiento no debería ser un problema, incluso si los encabezados de bloque deben mantenerse en la memoria.

[15] En el Anexo 5 se presenta una breve explicación de este concepto.

Figura N° 7: Verificación de pagos simplificada



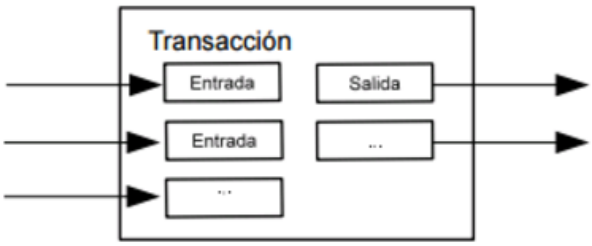
Fuente: Traducción de figura original de Nakamoto (2008)

Como tal, la verificación es confiable a medida que los nodos honestos controlen la red, pero se vuelve más vulnerable si la red es dominada por un atacante. Mientras los nodos de la red puedan verificar las transacciones por sí mismos, el método simplificado puede ser engañado por transacciones fabricadas por un atacante mientras éste pueda dominar la red. Una estrategia para protegerse es aceptar alertas de los nodos de la red cuando detecten un bloque inválido, pidiéndole al usuario que se baje el bloque completo y las transacciones alertadas para confirmar la inconsistencia. Los negocios que reciben pagos frecuentemente, querrán ejecutar sus propios nodos para tener una seguridad más independiente y una verificación más rápida.

5.7 Combinación y división de valor

Si bien es posible manipular monedas individualmente, sería difícil hacer una transacción por cada centavo en una transferencia. Para permitir que el valor sea dividido y combinado, las transacciones contienen múltiples entradas y salidas. Normalmente habrá una sola entrada de una transacción anterior más grande o múltiples entradas que combinen cantidades más pequeñas y como máximo dos salidas: una para el pago y otra que devuelva el cambio, si es el caso, al remitente (emisor). Cabe señalar que una transacción puede depender de varias transacciones, y esas a su vez depender de muchas más. Lo anterior se ilustra en la Figura N° 8.

Figura N° 8: Combinación y división de valor en una transacción



Fuente: Traducción de figura original de Nakamoto (2008)

5.8 Seguridad

Se considera el escenario en el que un participante atacante intenta generar una cadena alterna más rápido que la cadena honesta. Aún si esto se lograse, no abriría el sistema a cambios arbitrarios, tales como crear valor de la nada o tomar dinero que nunca le perteneció. Los nodos no aceptarían una transacción inválida como pago, y los nodos honestos nunca aceptaran un bloque que las contenga. Un participante atacante puede únicamente intentar cambiar solo sus propias transacciones para retomar dinero que ha gastado recientemente, es decir, la única forma de vulnerar el sistema sería con intentos de realizar doble gasto. En otras palabras, un atacante puede hacer creer al beneficiario que se le pagó durante un rato, para luego cambiar la transacción y pagarse a sí mismo de vuelta una vez que ha pasado un tiempo.

Becker et al. (2013) sostiene que mientras la mayoría de los usuarios sean honestos, ningún atacante estará en la posición de entregar la capacidad computacional necesaria para cambiar el orden temporal a su ventaja. El autor asegura que modificar una transacción realizada una hora antes, es decir, alrededor de cinco o seis bloques en el pasado, del bloque que la contiene no sólo requeriría recrear este bloque, sino también todos los subsiguientes, ya que el *hash* del bloque alterado es parte del siguiente. Por esta razón, alterar bloques anteriores de la cadena se vuelve computacionalmente imposible rápidamente.

6. Operaciones en sistema de Bitcoin con tecnología *blockchain*

De acuerdo a Möser et al. (2013), Bitcoin puede describirse como un sistema de contabilidad distribuido en el que las cuentas están asociadas con claves públicas en un esquema de cifrado asimétrico. El conocimiento de la clave privada correspondiente permite a los titulares de cuentas crear firmas digitales, demostrando así su elegibilidad para acceder a su cuenta.

Para mayor claridad, imagine un fichero de texto con dos columnas, donde en una columna pone un identificador (ejemplo “xyz”) y en la otra un número (ejemplo “87”). Es decir “xyz” le corresponde “87”. Esto es lo que hace la función *hash* descrita anteriormente.

Ahora, imagine que ese fichero pudiera estar en miles de computadores duplicado, con la seguridad de que nadie lo puede alterar individualmente pero cuando legítimamente se debe alterar algo, en cuestión de segundos, todos se sincronizan. Aunque uno de los miles de ordenadores desapareciese de la red no pasaría nada. Esto es lo que consigue *blockchain* y lo que en esencia busca: un registro distribuido resistente a la sincronización y sin necesidad de confianza entre los miembros que la conforman.

Una cadena de bloques es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está distribuido o es compartido entre muchas partes diferentes. En otras palabras, *blockchain* es un libro de contabilidad distribuido que permite transportar valor.

Este libro mayor solo puede ser actualizado a partir del consenso de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada. En el caso particular del Bitcoin, la cadena de bloques contiene un registro certero y verificable de todas las transacciones que se han hecho en su historia.

Lo que se plasma en el *blockchain* no puede desaparecer jamás. *Blockchain* es un registro inmutable y permanente. Se trata de una base de datos que solo permite escritura. No se puede modificar ni borrar nada de ello, solo añadir, y todo ello bajo consenso.

Gracias al concepto de consenso distribuido se puede crear un registro incorruptible de eventos pasados y presentes del mundo digital. Además, esto se logran sin comprometer la privacidad de los usuarios. Así, es posible registrar que el evento en cuestión ha tenido lugar y que lo ha hecho correctamente sin explicitar detalles concretos sobre el tipo de evento o las partes involucradas.

A continuación, se describen en detalle las principales operaciones que se realizan en el sistema Bitcoin, posibilitadas gracias a la tecnología de cadena de bloques.

6.1 Formación de cadena de bloques

La cadena de bloques es un registro de todas las transacciones que tienen lugar y que luego son empaquetadas en bloques que los mineros se encargan de verificar. Una vez validados, estos bloques, que son paquetes (conjuntos) de transacciones, son incluidos en la cadena y distribuidos a todos los nodos que forman la red.

De acuerdo con Möser et al. (2013), el protocolo estipula que cualquier salida referenciada por una entrada se agota y no es posible volver a hacer referencia de ella. Esto evita que los usuarios gasten (utilicen) dos veces su dinero haciendo referencia a una salida en dos transacciones diferentes. Una dificultad al hacer cumplir esta regla es que Bitcoin es un sistema distribuido. Por lo tanto, el destinatario de una transacción puede no estar en conocimiento de si el remitente ha hecho referencia a una salida en particular en otra transacción anterior.

Por esta razón, Bitcoin mantiene un registro probabilísticamente consistente de todas las transacciones denominado cadena de bloques. Los bloques son estructuras de datos que encapsulan transacciones junto a una referencia al bloque anterior, formando así una cadena. Los conflictos se resuelven usando un esquema de prueba de trabajo. Los bloques se consideran válidos sólo si todas sus transacciones son válidas y si son acompañadas por la solución de un problema computacional intensivo parametrizado por este bloque. Si bien la solución es difícil de encontrar, su validez puede ser fácilmente verificada.

Becker et al. (2013) explica que el orden temporal es establecido por la cadena de bloques. Los bloques recogen transacciones combinadas con un *hash* del bloque anterior, creando así una cadena. Un bloque es válido sólo si exhibe una propiedad especial que demuestra que se ha puesto una cierta cantidad de trabajo en su creación. En cuanto a la función *hash* correcta, esta sólo se puede lograr al probar aleatoriamente muchos valores diferentes de *nonce*. Así, la probabilidad de encontrar un bloque depende del número de ensayos. La dificultad del proceso se puede ajustar globalmente cambiando el número de ceros iniciales que debe tener el *hash*. Los ajustes regulares aseguran que los nuevos bloques se encuentren en promedio cada diez minutos.

Un gran número de mineros tratan permanentemente de encontrar tales soluciones utilizando poder computacional. Como se afirmó anteriormente, la dificultad del problema se adapta regularmente de tal manera que todos los mineros en conjunto encuentran una solución en promedio cada diez minutos. Quien encuentra la solución recibe una recompensa monetaria que se

paga en forma de una nueva transacción que no tiene una salida referenciada: una transacción de moneda base.

Por lo tanto, a través de la cadena de bloques, los usuarios acuerdan colectivamente el orden temporal de las transacciones según lo definido por el orden de los bloques que las contienen. Así, los usuarios asumen que la cadena de bloques más larga es la válida. Además, cualquier usuario del sistema Bitcoin puede mantener una copia local de la cadena de bloques y resolver los conflictos creyendo en la cadena más larga. La razón es que la cadena más larga debe haber sido creada por la mayoría de los mineros. Por lo tanto, ningún atacante puede ganar el control sobre la cadena de bloques a menos que logre obtener control sobre más poder de cálculo que todos los demás mineros en conjunto.

6.2 Proceso de creación de bloques: el trabajo de minería

En cualquier sistema monetario tradicional, la autoridad monetaria simplemente imprime más dinero cuando así lo estima necesario. En lo que respecta a Bitcoin, el dinero no se crea, sino que se descubre.

Para esto, miles de ordenadores de todo el mundo minan (buscan) Bitcoins compitiendo unos con otros. Los mineros obtienen Bitcoins como recompensa a la resolución de un problema matemático en el que cada 10 minutos compiten miles de nodos, siendo la red de computación más potente que hoy en día existe.

Este reto matemático siempre es igual en su proceso, pero las variables son diferentes y solo es posible de resolver probando números al azar sin parar hasta dar con el resultado que se busca en ese momento. El primero que lo consiga se lleva la recompensa. Esto genera competencia y búsqueda de eficiencia mejorando los ordenadores para este objetivo.

6.2.1 Proceso de minería de Bitcoins

Los usuarios envían Bitcoins de forma constante de un lado a otro, pero a menos que alguien registrase todas estas transacciones, nadie podría comprobar quién ha pagado qué en un momento determinado. La red de Bitcoin gestiona esto dejando constancia de todas las transacciones llevadas a cabo en un periodo determinado en una lista, llamada bloque.

El trabajo de los mineros es confirmar esas transacciones y escribirlas en el libro mayor. Este libro mayor es una larga lista de bloques conocida como cadena de bloques.

Ésta puede utilizarse para explorar o consultar cualquier transacción que haya tenido lugar entre direcciones de Bitcoin en cualquier lugar. Cada vez que se crea un nuevo bloque, se añade a la cadena, creando una lista cada vez mayor con todas las transacciones que se han hecho en toda la historia de la red de Bitcoin. Una copia actualizada en tiempo real de los bloques se descarga en cada ordenador o nodo que esté aportando poder computacional a la red.

Este libro mayor, que se sostiene de forma digital, tiene la tarea de generar confianza. Para esto, al crearse un bloque de transacciones, los mineros dan lugar a él siguiendo el proceso descrito a continuación: Recogen la información del bloque y le aplican una fórmula matemática, convirtiéndolo en algo diferente. Esta nueva pieza de información es más corta y en apariencia es

una secuencia de números y letras aleatoria denominada técnicamente *hash*. Este *hash* se almacena con el bloque, al final del mismo, en último lugar en la cadena en ese momento.

Los *hashes* tienen algunas propiedades interesantes. Es fácil producir un *hash* de un conjunto de datos como un bloque de transacciones, pero es prácticamente imposible acceder a los datos simplemente con el *hash*. En otras palabras, mientras que es muy fácil producir un *hash* de un gran conjunto de datos, cada uno es único. Esto produce que, si se cambia un único carácter del bloque, el *hash* cambiará por completo.

Los mineros no solo usan las transacciones de un bloque para generar un *hash*. También se utilizan otros datos. Uno de estos datos es el *hash* del último bloque añadido a la cadena. Debido a que el *hash* de cada bloque se produce utilizando el *hash* del bloque inmediatamente anterior, se convierte en una versión digital de un sello de lacre.

Con este encadenamiento, es posible confirmar que un bloque y todo aquel que va a continuación es legítimo. Si alguien intenta falsificar una transacción cambiando un bloque que ya había sido almacenado en la cadena, el *hash* de ese bloque cambiaría. Así, si un usuario intentase comprobar la autenticidad del bloque aplicando la función matemática encima, se encontrarían con que el *hash* sería distinto de aquel que ya está almacenado con ese bloque en la cadena y, como consecuencia, el bloque sería automáticamente identificado como falso.

6.2.2 Competencia por descubrir Bitcoins

De acuerdo a lo anterior, los mineros van sellando los bloques. Todos ellos compiten por ser quien realiza este sellado, utilizando un software escrito específicamente para minar bloques. Cada vez que un minero logra crear un *hash* con éxito (es decir, logra realizar el sellado), se lleva una recompensa en Bitcoins, la cadena de bloques se actualiza y todo el mundo en la red es notificado de ello. Esta recompensa en Bitcoins es el incentivo para seguir minando y permitir que se sigan llevando a cabo transacciones. Es decir, como se explicó anteriormente, existen incentivos a supervisar el sistema.

El problema es que es muy fácil producir un *hash* directamente a partir de un conjunto de datos. Ya que para un ordenador resulta muy fácil producirlo, la red de Bitcoin ha de hacerlo más difícil, ya que de otra manera todo el mundo estaría creando *hash* de centenares de bloques de transacciones cada segundo y todos los Bitcoins se minarían (descubrirían) en minutos.

El protocolo de Bitcoin no acepta ningún *hash* con formato antiguo. Éste exige que el *hash* de cada bloque sea de una manera determinada, debiendo tener un número de ceros determinado al principio. Por lo anterior, no hay manera de saber cómo va a ser un *hash* antes de producirlo y, tan pronto se incluya un nuevo dato, el *hash* será totalmente diferente.

Se asume que los mineros no interaccionan con los datos referentes a transacciones que hay dentro de cada bloque, pero deben cambiar los datos que están utilizando para crear un *hash* diferente. Para hacerlo, acuden a otro trozo de información aleatorio que se conoce como *nonce* y que se utiliza junto a los datos de la transacción para crear un *hash*. Si el *hash* no se ajusta al formato exigido, el *nonce* se cambia y se prueba de nuevo creando un nuevo *hash* de forma iterativa.

Cabe destacar que puede llevar varios intentos encontrar un *nonce* que funcione y que todos los mineros de la red están intentando hacerlo al mismo tiempo. De hecho, lleva millones de intentos,

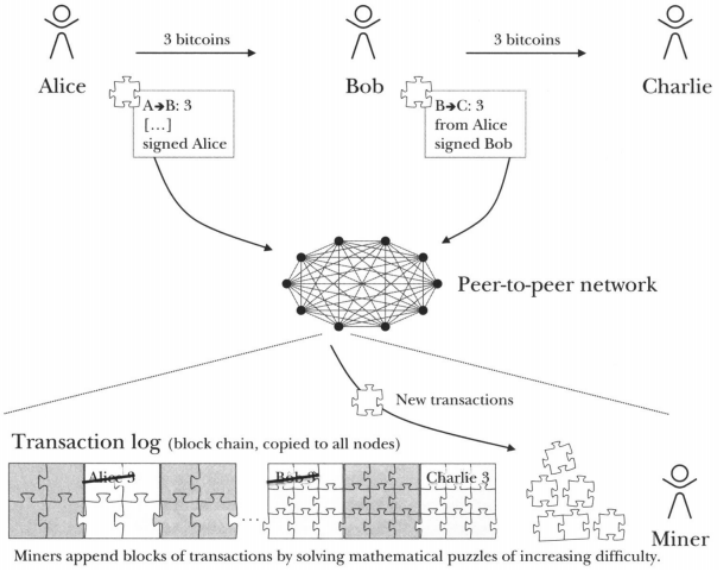
realizados por miles de ordenadores que intentan dar con el número que devuelva el patrón que en ese momento se está exigiendo.

6.3 Transacciones en sistema Bitcoin

Un elemento fundamental del sistema Bitcoin es la transacción[16], la cual se utiliza para transferir dinero entre cuentas. De acuerdo a Möser et al. (2013), cada transacción consiste en una lista de salidas, que son cantidades monetarias y claves públicas que identifican la cuenta de destino; y una lista de entradas, que son referencias a salidas de transacciones anteriores. La semántica de una transacción es que las entradas consumen por completo las salidas referenciadas (de transacciones anteriores). Las entradas reducen el saldo de la cuenta del remitente, mientras que las salidas (de la transacción actual) aumentan el saldo de la cuenta del receptor. Para asegurarse de que sólo el propietario puede retirar fondos de una cuenta, cualquier transacción se combina con firmas digitales correspondientes a las claves públicas referenciadas en las entradas.

Cabe destacar que los Bitcoins se registran como transacciones, es decir, se registran los cambios de propiedad de cada moneda. Siguiendo el ejemplo de Böhme et al. (2015), el usuario Charlie no "mantiene" simplemente tres Bitcoins. Por el contrario, Charlie participa en una transacción públicamente verificable mostrando que recibió tres Bitcoins de Bob. Charlie pudo comprobar que Bob podía hacer ese pago porque había una transacción anterior en la que Bob recibió tres Bitcoins de Alice y no hubo ninguna transacción previa en la que Bob transfirió estos tres Bitcoins. En el esquema que se presenta a continuación, se ilustran estas interacciones.

Figura N° 9: Flujo y validación en una transacción con el sistema Bitcoin



Fuente: Böhme et al. (2015)

[16] En el Anexo 6 se presenta una infografía que resume cómo opera la tecnología *blockchain* en el caso particular de una transacción con la moneda virtual Bitcoin.

De hecho, cada Bitcoin se puede remontar fácilmente a través de todas las transacciones en las cuales fue utilizado, y así hasta el comienzo de su circulación. Todas las transacciones de Bitcoin son de acceso público (libre consulta) y legibles por todos en los registros almacenados en una estructura de datos ampliamente replicada. En general, las transacciones se ordenan recursivamente al tener como entrada de una transacción (la fuente de los fondos) la salida de una transacción anterior. (Utilizando el ejemplo anterior, la transacción podría revelar que Bob paga a Charlie usando Bitcoin que recibió de Alice.)

Bitcoin se basa en dos tecnologías fundamentales de la criptografía: criptografía de clave público-privada para almacenar y gastar (utilizar) dinero; y validación criptográfica de transacciones. La criptografía de clave público-privada estándar permite que cualquier usuario cree una clave pública y una clave privada asociada. Las claves públicas están diseñadas para ser ampliamente compartidas, por eso su nombre. Los mensajes cifrados con una clave pública sólo pueden ser descifrados por alguien que posea la clave privada correspondiente, lo que permite a cualquiera cifrar un mensaje que sólo el destinatario especificado puede leer. Del mismo modo, los mensajes cifrados con una clave privada sólo se pueden descifrar con la clave pública correspondiente, permitiendo que un remitente especificado cree un mensaje que se puede confirmar que es auténtico. En Bitcoin, fundamentos de cifrado similares autentican instrucciones para transferir dinero a otros participantes. Dicha instrucción se cifra usando la clave privada del remitente, confirmando para todos que la instrucción de hecho vino del remitente.

Siguiendo con el ejemplo anterior, supongamos que Alice tiene tres Bitcoins que quiere dar a Bob. Ella publica un mensaje en la red de Bitcoin indicando que ella está transfiriendo tres de sus Bitcoins existentes, junto con una referencia a la transacción donde ella había recibido esos Bitcoins. Parte de este mensaje es cifrado por la clave privada de Alice para probar que la instrucción vino de ella, en un método similar a una firma en un cheque de papel. Más tarde, si Bob quiere enviar Bitcoins a Charlie, publica un mensaje, de nuevo cifrado con su clave privada, indicando que él consiguió sus Bitcoins de Alice y lo que quiere enviar a quién. La red Bitcoin identifica a Alice, Bob y Charlie sólo por sus claves públicas, que operan como los números de cuenta en el sistema tradicional.

Cada nueva transacción que se publica en la red de Bitcoin se agrupa periódicamente en un bloque de transacciones recientes. Para asegurarse de que no se han insertado transacciones no autorizadas, el bloque en sí se compara con el bloque más reciente validado y publicado por los nodos, lo que produce una secuencia enlazada de bloques, o una cadena de bloques. Un bloque nuevo se agrega a la cadena aproximadamente cada diez minutos. Con esta estructura de datos, cualquier usuario de Bitcoin puede verificar si una transacción anterior efectivamente ocurrió.

Mantener el registro de transacción operativo y actualizado es un bien público, ya que es la base de todo el sistema Bitcoin. Para incentivar a los usuarios a mantenerlo, el sistema Bitcoin otorga periódicamente premios de Bitcoins recién acuñados al usuario que resuelve un rompecabezas matemático que se basa en el contenido preexistente del bloque (esto previene la manipulación del bloque y por lo tanto la modificación de transacciones anteriores) y que sólo puede ser resuelto por métodos computacionalmente intensivos que incluyen un componente aleatorio. Por lo tanto, para un poder computacional mayor es más probable resolver un problema dado y resolverá un mayor número de estos problemas, pero al tener un componente aleatorio, la velocidad por sí sola no garantizará el éxito.

Al resolver el rompecabezas, el usuario publica un bloque que contiene una prueba de trabajo de que se llevó a cabo una solución junto con todas las transacciones observadas que han tenido lugar

desde que se anunció la última solución de rompecabezas y una referencia al bloque completo anterior. Después de que otros usuarios verifiquen la solución, comienzan a trabajar en un nuevo bloque que contiene nuevas transacciones pendientes. Este proceso se denomina trabajo de minería y recursivamente asegura que el ordenamiento histórico total sobre todos los bloques (la cadena) sea acordado por toda la red.

Una transacción de Bitcoin no se confirma (y por lo tanto no es definitiva) hasta que se ha agregado a la cadena de bloques de consenso. Los lotes de transacciones se agregan cada diez minutos en promedio. Sin embargo, los mineros están continuamente trabajando en la adición de bloques de transacciones basándose en las transacciones anteriores. Al presentar continuamente sus soluciones a los rompecabezas, con la nueva cola asociada de la cadena de bloques, los mineros están efectivamente "votando" por el registro (orden) correcto de las transacciones y, de esa manera, verificar y validar las transacciones. En algunos casos, se agregará un lote de transacciones a la cadena de bloques, pero luego de unos minutos se alterará debido a que la mayoría de los mineros alcanzaron una solución diferente. Normalmente, las fuentes recomiendan considerar una transacción de Bitcoin como definitiva sólo después de seis confirmaciones, para asegurar que la transacción se registra efectivamente de forma permanente en la cadena de bloques. Si bien esto proporciona mayor seguridad, crea un retraso aproximado de una hora antes de que una transacción Bitcoin finalmente sea validada.

A medida que los mineros actualizan la cadena de bloques, sus esfuerzos computacionales conllevan costos significativos. En particular, los cálculos computarizados de prueba de trabajo son muy intensivos en energía, consumiendo más de 173 megawatts de electricidad de forma continua. Como referencia, esa cantidad tiene un valor de US$ 178 millones por año a los precios promedio de la electricidad residencial en Estados Unidos. Estos costos computacionales han crecido abruptamente y pueden aumentar aún más debido a que el protocolo de Bitcoin ajusta automáticamente la dificultad del rompecabezas de modo que el intervalo de tiempo entre dos bloques permanezca aproximadamente diez minutos. A medida que más poder de cálculo se une al sistema Bitcoin, los rompecabezas se vuelven automáticamente más complejos, aumentando los requerimientos de poder computacional y de energía.

Exigir a los mineros que resuelvan un rompecabezas ayuda a evitar ciertos tipos de fraude. En principio, un sistema como Bitcoin podría validar las transacciones usando un consenso simple por mayoría de votos, emitidos por una mayoría de los usuarios conectados capaces de afirmar que una transacción dada efectivamente ocurrió. Pero entonces, un atacante podría vulnerar el sistema mediante la creación de numerosas identidades falsas. En respuesta a esto, el protocolo Bitcoin hace que sea costoso enviar votos falsos. De acuerdo con la arquitectura abierta de Internet, cualquier persona puede conectar varios ordenadores al sistema Bitcoin. Pero votar sobre la autenticidad de una transacción requiere primero trabajar para resolver un rompecabezas matemático que es computacionalmente difícil de resolver (aunque fácil de verificar). Resolver el rompecabezas proporciona una prueba de trabajo. Así, en lugar de "una persona, un voto", Bitcoin implementa el principio de "un ciclo computacional, un voto". A través de este diseño, el mecanismo de prueba de trabajo simultáneamente desalienta la creación de numerosas identidades falsas y también proporciona incentivos para participar en la verificación de la cadena de bloques.

7. Principales diferencias entre el sistema tradicional y el sistema con la tecnología *blockchain*

A continuación, se presentan dos elementos que resultan ser las principales diferencias entre el sistema de transacciones bancarias tradicional y el sistema de Bitcoin que utiliza la tecnología *blockchain*. Éstos son el carácter irreversible de las transacciones y el nivel de privacidad de los usuarios y las operaciones que realizan.

7.1 Irreversibilidad de las transacciones

El dinero en esencia no es reversible. Todas las posibilidades de reversibilidad provienen de terceras personas, instituciones, intermediarios y empresas. Esta reversibilidad da espacio para el fraude y al mismo tiempo opera como protección contra éste, y es un servicio que se puede brindar a quienes usan y poseen dinero.

Debido a que en el sistema "puro" de Bitcoin no existen estas terceras partes[17], los usuarios que pagan con Bitcoin, corren el mismo riesgo que alguien que envía sus dólares físicos por correo.

Cuando por defecto se cuenta con un sistema con completa fungibilidad e irreversibilidad, como en el caso de Bitcoin, se asume siempre que una transacción es legítima. Es decir, no existe riesgo de que el dinero que se recibe sea falso o que te pueda ser quitado sin tu consentimiento. El riesgo de fraude con Bitcoin, de hecho, es menor al riesgo de fraude con cualquier otra forma de dinero fiduciario.

De hecho, como de expuso en la sección 3, no se podría usar dinero de haber alguna posibilidad de que éste te pueda ser quitado. Sólo será útil si las transferencias pueden ser completadas. Si esto no ocurre, como sucede en el sistema tradicional, entonces tiene sentido que aparezcan protocolos de protección contra el fraude y otros servicios de terceros constituidos en torno al dinero.

La irreversibilidad no es sólo una característica de Bitcoin, sino que es una cualidad fundamental, necesaria para su propia existencia. Gracias a la irreversibilidad, la gente puede ser realmente libre de transar sin interferencias.

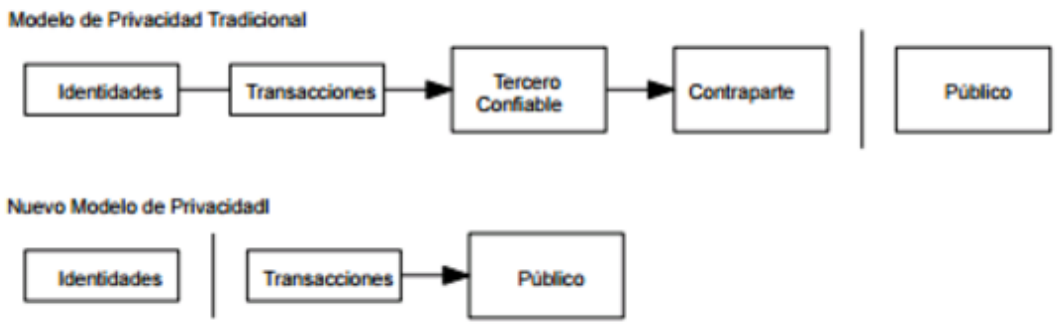
7.2 Privacidad

El modelo bancario tradicional logra su nivel de privacidad al limitar el acceso a la información a las partes involucradas y a la tercera parte confiable. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún se puede mantener rompiendo el flujo de información en otro lugar: manteniendo anónimas las claves públicas. El público puede ver

[17] Actualmente, existen empresas que ofrecen servicio de *escrow* o depósito en garantía para las transacciones de Bitcoins entre desconocidos. Todas las formas en las que se utiliza el dinero y se obtiene protección contra el fraude, son implementables con Bitcoin, porque en realidad no son inherentes al propio dinero, sino servicios en torno a éste. En el Anexo 7 se presenta un esquema con el fin de clarificar esta idea.

que alguien está enviando una cierta cantidad a otra persona, pero sin información que relacione la transacción con nadie en particular. Esto es similar al nivel de información que se muestra en las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales (la "cinta"), son públicos, pero sin decir quiénes son las partes. En la Figura N° 10 se ilustra la diferencia de privacidad entre ambos sistemas.

Figura N° 10: Diferencias en privacidad entre sistema bancario tradicional y sistema Bitcoin con tecnología *blockchain*



Fuente: Traducción de figura original de Nakamoto (2008)

Esto explica por qué Bitcoin se ha utilizado para llevar a cabo transacciones ilegales ya que, a pesar del acceso público y libre al libro mayor, la identidad y privacidad de sus usuarios está garantizada si así se requiere.

No obstante, son inevitables algunos tipos de asociación con transacciones de múltiples entradas, las que pueden revelar que sus entradas pertenecen al mismo dueño. El riesgo estaría en que, si el dueño de una clave se revela, entonces el enlazado podría revelar otras transacciones que pertenecieron al mismo dueño.

8. Regulación del uso de Bitcoin

En relación con el ámbito legal, Gutiérrez (2015) sostiene que una de las mayores preocupaciones es el carácter pseudoanónimo que tiene Bitcoin, lo que lo convierte en una herramienta potencialmente útil para actividades ilícitas como por ejemplo el lavado de dinero, la evasión de impuestos, utilización para la compra y venta de productos ilegales y el financiamiento de grupos terroristas. Además, los usuarios no cuentan con un respaldo o una entidad a la que acudir en caso de estafas y/o perjuicios ocasionados por terceros.

En términos políticos, el autor sostiene que el uso de Bitcoin tiene principalmente dos implicancias que producen que gran parte de los gobiernos y bancos centrales del mundo lo resistan. La primera, y de una mayor importancia si el Bitcoin llegase a ser una moneda de uso masivo, es la imposibilidad de su manipulación por parte de los gobiernos. Las políticas monetarias expansivas y contractivas utilizadas por los gobiernos para controlar distintas situaciones económicas no se podrían llevar a cabo sobre una economía que use principalmente Bitcoins. De momento, hay consenso en que los

volúmenes de operaciones no son lo suficientemente grandes como para desestabilizar una moneda como la europea, pero esto podría cambiar en el futuro con el Euro u otra divisa.

La otra gran preocupación es la incapacidad impositiva de los gobiernos sobre el Bitcoin. Esta problemática está compuesta a su vez por dos aristas. La primera es la incapacidad del gobierno de registrar y aplicar impuestos sobre todas las transacciones realizadas con Bitcoins, lo que se ve dificultado en gran medida por el carácter pseudoanónimo de éste mencionado anteriormente. La segunda arista viene dada por la elección del tipo de tasas impositivas que se debería aplicar. La discusión gira entorno a si se deben aplicar tasas impositivas correspondientes a operaciones realizadas con dinero, o bien, tasas aplicadas a los activos financieros. Dependiendo de cómo sea gravada la moneda digital, los efectos en su uso y el volumen de transacciones realizadas podrían variar.

Cabe mencionar que actualmente no hay consenso global sobre la legalidad de Bitcoin ni sobre qué tasa impositiva aplicar. Por un lado, están los países que han optado por prohibir el Bitcoin y hacer ilegal su uso. Entre estos países están Islandia, India, Tailandia, Bolivia y Ecuador.

Por el otro lado, están los países en que se está discutiendo sobre el uso de Bitcoin por parte de los bancos centrales y sobre qué tasa impositiva aplicar a las transacciones realizadas con la criptomoneda. En relación a esto último y a modo de ejemplo, si bien China aconsejó a sus bancos no comerciar con Bitcoins, el Banco Popular de China ha realizado pruebas de su propio prototipo de criptomoneda, yendo contra los principios fundamentales de ésta.

En el caso de Alemania, el gobierno declaró en junio de 2013 que el Bitcoin sería tratado como una actividad comercial y que estaría sujeto a impuestos relacionados con las rentas obtenidas, a menos que estas fueran mantenidas por un periodo superior a un año. En agosto del mismo año, el primer ministro alemán reconoció al Bitcoin como una unidad de cuenta equivalente a una “moneda privada” en la ley alemana, lo que significa que además de estar sujeto a impuestos sobre las rentas obtenidas, tiene que tributar bajo los tipos de interés de ventas (IVA). Del mismo modo, la regulación en Reino Unido y España exigen el pago del IVA a las transacciones de la criptodivisa.

Por su parte, si bien el gobernador de la Reserva Federal de Estados Unidos sostuvo que el banco central de Estados Unidos no está considerando adoptar ni implementar una moneda digital, a partir del 2015 Estados Unidos reconoce el Bitcoin como un *commodity* al igual que el petróleo o el oro.

Finalmente, en el otro extremo, Japón ha aceptado oficialmente el Bitcoin como medio de pago y se estima que, en Tokio, a fin de este año, más de 22.000 negocios estarán habilitados para recibir pagos con esta moneda.

En Chile, el Bitcoin y otras criptomonedas siguen siendo poco conocidos como instrumentos de ahorro o inversión, lo que constituye una barrera que impide su mayor expansión en el mercado interno, razón por la que sus volúmenes de transacción en los últimos meses han seguido siendo bajos. A nivel de la industria local, las transacciones rondan los US$7 millones mensuales, cifra que aún está muy lejos de países como Japón, en que se transan alrededor de US$100 millones diarios. Como referencia, a nivel global, el volumen de transacción de criptomonedas está en torno a los US$5 mil millones al día.

Consultado sobre la regulación de estas criptodivisas, el Banco Central precisó que las monedas virtuales no cuentan con un reconocimiento legal o reglamentario específico en nuestro país y que la actividad de compraventa o intermediación de estas no está sujeta a la potestad regulatoria de este organismo, pero agregó que en la medida que las empresas dedicadas a la intermediación de monedas virtuales efectúen operaciones de cambio internacionales, éstas podrían quedar sujetas a las facultades que le competen a la institución en materia cambiaria.

Por su parte, la Unidad de Análisis Financiero (UAF) sostiene que este mercado está fuera de su perímetro regulatorio, debido a que en Chile aún no se define legalmente qué es un Bitcoin, ni quién debe regularlo.

Los efectos de una regulación sobre el Bitcoin podrían ser trascendentales en su desarrollo futuro. Una regulación relacionada con las actividades ligadas al Bitcoin en su formato actual implicaría restricciones sobre la facilidad de acceso al mundo financiero que la criptomoneda permite hoy en día. Esta regulación aumentaría la seguridad a la hora de operar utilizando terceras partes por lo que resultaría beneficioso para el desarrollo del sistema y para el público general. Otro efecto potencial de esta regulación es la toma de posesión de las operaciones en Bitcoin por parte de los operadores financieros ya afianzados en nuestra sociedad.

9. Uso de Bitcoin como medio de cambio e impacto potencial en mercados financieros

Como se ha expuesto, Bitcoin posee gran parte de los elementos necesarios para convertirse en una moneda independiente de bancos centrales y entidades reguladoras. Sin embargo, actualmente existen grandes obstáculos a su funcionalidad como moneda. La principal es la volatilidad de precios que presenta debido a los movimientos especulativos que ha sufrido. Esto le imposibilita representar un depósito de valor seguro y formar una unidad de medida sin riesgo para los comercios. Estos inconvenientes impiden la aceptación general de la criptomoneda entre quienes participan en el mercado y no están dispuestos a asumir tales riesgos de fluctuación.

A su vez, esta gran volatilidad refuerza su condición de activo financiero, debido a su falta de funcionalidad como moneda. Pero también denota los grandes hitos que ha de cumplir para convertirse en una. Estos son la eliminación de la volatilidad y la proliferación de usuarios que lo utilicen como medio de cambio y no como medio de especulación.

La volatilidad parece estar en un proceso de reducción. De todas formas, este estado es temporal ya que la formación de burbujas en un sistema como Bitcoin, en el que no existe control gubernamental, depende completamente del estado anímico del mercado. Así también, el uso como moneda está amenazado por un mayor control impositivo sobre los beneficios producidos por la compra venta de Bitcoin. Esos tipos impositivos además de aumentar el coste de operar en Bitcoin aumentan la percepción del mismo en la sociedad como un activo financiero.

Por lo tanto, para la superación de estos hitos, Bitcoin necesitaría contar con el respaldo de un sistema financiero y regulación legal que actualmente están en un estado muy prematuro, pero que muestran una tendencia de crecimiento. Sin embargo, la consecución de estos hitos y la verdadera consolidación como moneda acarrearía importantes efectos en los sistemas políticos, económicos y

legales actuales. Estos efectos se refieren principalmente a la reducción del poder estatal y a la dificultad de emprender acciones legales (debido a su carácter pseudoanónimo) por lo que surgirían numerosas presiones sobre la moneda digital con el fin de evitar estos efectos. Para un cambio monetario total hacia Bitcoin haría falta poyo económico, social y político del mismo. De acuerdo a lo anterior, este apoyo se plantea, de momento, imposible.

Por lo tanto, debido a las presiones ejercidas por parte de los grandes gobiernos, Bitcoin no podría llegar a conformar una moneda que sustituya a las principales divisas mundiales como el Dólar, el Yen o el Euro, entre otras. Sin embargo, la criptomoneda alberga el potencial para convertirse en una moneda alternativa a estas formas de dinero convencional. Esto produciría un desplazamiento de pequeñas monedas cuyo soporte gubernamental y aceptación es reducido, y que por lo tanto sufren de constantes fluctuaciones y riesgo de pérdida de valor. La falta de un respaldo de confianza para mantener su valor en el caso de Bitcoin, sería compensada por la falta de respaldo gubernamental de estas monedas menores.

Las monedas virtuales permiten que las personas intercambien valor entre ellas sin la necesidad de intermediarios. De esta forma, se evitan costos en comisiones para, por ejemplo, enviar dinero a cualquier parte del mundo. Esto podría revolucionar el sistema financiero completo, al permitirle a personas de escasos recursos o sin acceso a crédito, enviar dinero a cualquier parte del mundo por costos menores a los actuales, o bien, protegerse de los altos niveles de inflación y pérdida de valor de las monedas locales.

Con respecto a esto último, países como Argentina y Venezuela vieron una gran oportunidad en el Bitcoin como una vía de internacionalizar los ahorros en moneda local. El mercado informal permitió rápidamente acceder a la compra y venta de Bitcoin, pero no pasó mucho tiempo para que corredores y centros de intercambio regionales abrieran sus portales en internet permitiendo comprar y vender en moneda nacional.

Reforzando la idea anterior, Hileman (2015) construye un Índice de Mercado Potencial para Bitcoin con el fin de estudiar qué países tendrían mayor utilidad al adoptarlo. El índice utiliza un conjunto de datos con 40 variables relacionadas con las funciones básicas actuales de Bitcoin, las cuales son reserva de valor, medio de pago o cambio y plataforma tecnológica. Estas variables se agrupan en los siete subíndices igualmente ponderados del índice: penetración de tecnología, remesas internacionales, inflación, tamaño de economía, represión financiera, crisis financieras históricas y penetración de Bitcoin. De acuerdo a este índice se construye un ranking para 178 países. Los resultados muestran que los países en que la criptomoneda tiene mayor potencial de adopción son Argentina, Venezuela y los países que comprenden la región de África Subsahariana.

10. Potencial de tecnología *blockchain*

Mientras las monedas digitales se roban el protagonismo en el presente, las entidades que tradicionalmente han operado en el mercado de divisas y arbitrajes, como bolsas y bancos, han empezado a trabajar en distintas aplicaciones basadas en la tecnología detrás de Bitcoin.

Las aplicaciones para este sistema podrían ser variadas. A nivel global, los bancos se encuentran trabajando en, por ejemplo, simplificar los procesos de entrega de créditos hipotecarios a través de *blockchain*, lo que permitiría reducir los tiempos de otorgamiento.

Sólo en la banca, se estima que a nivel mundial la tecnología *blockchain* podría generar ahorros por US$20 mil millones. Anualmente, los costos de las transacciones que podrían ser reducidas con la nueva tecnología están entre los US$65 mil y los US$80 mil millones.

Una de sus aplicaciones emergentes más relevantes tiene que ver con lo que se conoce como "contratos inteligentes" o *smart contracts*. Éstos consisten en la capacidad para confiar en una red distribuida la confirmación de que un contrato de cualquier tipo ha sido cumplido sin revelar ningún tipo de información confidencial sobre las partes y/o naturaleza de la transacción.

Esto serviría, por ejemplo, para liberar un pago a un *freelance* al que has subcontratado cuando termine su trabajo o para algo tan trivial como que tu lavadora compre por sí misma detergente una vez que detecte que se ha acabado. Las implicaciones que esto tiene en relación a la confianza y transparencia a la hora de realizar transacciones de cualquier tipo son sencillamente inmensas.

Almacenamiento en la nube distribuido

Los servicios de almacenamiento en la nube como Dropbox o Google Drive son centralizados y al usarlos se confía en que un único proveedor responda por los datos que se almacenan en él.

Storj es una *startup* que está testeando en forma de beta un servicio que permite que esto se haga de forma distribuida utilizando una red basada en *blockchain* para aumentar la seguridad y hacer menos dependiente el servicio.

Patentes/registro de propiedad

Uno de los primeros servicios no financieros que se le ha dado a la cadena de bloques es la inclusión de información encriptada dentro de las transacciones. De esta manera, se puede crear un *hash* imposible de replicar que está asociado a un documento único almacenado fuera de la cadena de bloques.

Una empresa como Google, por ejemplo, podría probar que ha creado una tecnología en una fecha concreta sin necesidad de hacer una aplicación formal para registrar la patente. Así, podría vincular esos documentos internos al *hash* de una transacción realizada en ese momento y probar así que ellos han sido los primeros en desarrollarla.

Voto electrónico

No es difícil de imaginar al alto costo que conlleva crear papeletas, organizar toda la infraestructura necesaria para gestionar las votaciones y el posterior conteo.

Ya se han probado sistemas de voto electrónico, pero han sido incapaces de resistir ataques de *hackers* y de tener fallos a la hora de hacer el recuento con total precisión. *Blockchain* podría solucionar esto ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, infalsificable, a un coste prácticamente nulo y de acceso público.

Gobierno transparente

Con la tecnología *blockchain*, cualquier gobierno podría reflejar el estado de sus cuentas en tiempo real. Con una moneda como Bitcoin el gobierno solamente debería indicar cuál es la dirección que ellos gestionan, y desde ese momento, todos podrían observar el estado de las cuentas, qué entra y qué sale: hasta el último céntimo, en tiempo real y con costo cero.

Si en un momento dado hay un pago que se va a una dirección que no se puede justificar con una factura, los auditores y el público entero lo vería al instante. Además, se debe recordar que *blockchain* es una cadena, por lo que no es posible agregar algo en ella a posteriori para intentar falsear las cuentas del pasado.

Se puede pensar incluso más allá poniendo sobre la mesa historiales médicos, votaciones, registros de propiedad, actas matrimoniales o litigios gestionados por la cadena de bloques. Eventualmente, todo conjunto de datos y transacción digital podría dejar su huella dactilar allí, creando un rastro fácilmente auditable de todo evento digital que tenga lugar en la historia sin comprometer la privacidad de nadie.

11. Conclusiones

Las monedas virtuales permiten que las personas intercambien valor entre ellas sin la necesidad de intermediarios. De esta forma, se evitan costos en comisiones para, por ejemplo, enviar dinero a cualquier parte del mundo. Esto podría revolucionar el sistema financiero completo, al permitirle a personas de escasos recursos o sin acceso a crédito, enviar dinero a cualquier parte del mundo por costos menores a los actuales, o bien, protegerse de los altos niveles de inflación y pérdida de valor de las monedas locales.

Blockchain, la tecnología detrás de las criptomonedas, consiste en un sistema de transacciones electrónicas que no depende de la confianza en terceras partes o en intermediarios financieros. El sistema tradicional sin intermediación financiera presenta el riesgo del doble gasto y cuando se incorpora la intermediación, se pierde la irreversibilidad de las transacciones, lo que podría transformarse en un riesgo para algunos agentes.

Para superar este problema, *blockchain* presenta una red usuario-a-usuario que utiliza pruebas de trabajo para registrar una historia pública de transacciones y que rápidamente se hace irresoluble computacionalmente para un participante que quiera obtener ventaja cambiando este registro unilateralmente, siempre que los nodos honestos controlen la mayoría del poder de computacional.

La red es robusta por su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular y solo necesitan ser entregados bajo la base del mayor esfuerzo. Los nodos pueden ir y volver de la red a voluntad, aceptando la cadena de prueba de trabajo como prueba de lo que sucedió mientras estuvieron ausentes. Éstos votan con su poder computacional, expresando su aceptación de los bloques válidos al trabajar extendiéndolos, y rechazando bloques inválidos al rehusar trabajar en ellos. Cualquier regla necesaria o incentivos pueden hacerse cumplir con este mecanismo de consenso.

Cabe destacar que el potencial de *blockchain* va mucho más allá de la criptomoneda Bitcoin. La cadena de bloques sirve para llevar la contabilidad potencialmente de cualquier cosa. En otras palabras, *blockchain* es un libro de contabilidad distribuido que permite transportar valor como nunca antes se había podido hacer.

De forma paralela, es necesario señalar que el análisis de las innovaciones que han surgido dentro del marco del sistema bancario tradicional como respuesta a la irrupción de *blockchain* queda pendiente para una futura investigación. Entre éstas, podemos encontrar principalmente dos: la

primera, el surgimiento de las empresas *fintech*, que, a través del uso de las nuevas tecnologías, buscan realizar el trabajo de intermediación y proveer servicios financieros a los clientes a menor costo. La segunda, es la creación de una nueva regulación europea en materia de pagos que implica cambios fundamentales en la industria al dar acceso a terceros a la infraestructura de los bancos, denominada PSD2.

Finalmente, es posible afirmar que los efectos de una regulación sobre el Bitcoin podrían ser trascendentales en su desarrollo futuro. Una regulación relacionada con las actividades ligadas a Bitcoin en su formato actual implicaría restricciones sobre la facilidad de acceso al mundo financiero que Bitcoin permite hoy en día. Esta regulación aumentaría la seguridad a la hora de operar utilizando terceras partes por lo que resultaría beneficioso para el desarrollo del sistema y para el público general. Otro efecto potencial de esta regulación es la toma de posesión de las operaciones en Bitcoin por parte de los operadores financieros ya afianzados en nuestra sociedad.

Referencias

Becker, J., D. Breuker, T. Heide, J. Holler, H.P. Rauer y R. Böhme (2013). Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In *The Economics of Information Security and Privacy* (pp. 135-156). Springer Berlin Heidelberg.

Böhme, R., N. Christin, B. Edelman y T. Moore (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, *29*(2), 213-238.

Brito, J., H.B. Shadab y A. Castillo (2015). Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling.

Candelario, B. (2015). Bitcoin: Información Sobre Su Reglamento En Las Américas y Futuro Crecimiento. U. Miami Inter-Am. L. Rev., 47, 95.

De Filippi, P. (2014). Bitcoin: a Regulatory Nightmare to a Libertarian Dream. Browser Download This Paper.

Dodgson, M., D. Gann, I. Wladawsky-Berger, N. Sultan y G. George (2015). Managing Digital Money. Academy of Management Journal, 58(2), 325-333.

Dwyer, G.P. (2015). The Economics of Bitcoin and Similar Private Digital Currencies. Journal of Financial Stability, 17, 81-91.

European Banking Authority (2014). EBA Opinion on "Virtual Currencies".

Gutiérrez, P. (2015). El Bitcoin: ¿Presente y Futuro del Dinero? Sus Características e Implicaciones.

Harasic, V. (2014). It's Not Just About the Money: A Comparative Analysis of the Regulatory Status of Bitcoin Under Various Domestic Securities Laws. Am. U. Bus. L. Rev., 3, 487.

Hendrickson, J.R., T.L. Hogan y W.J. Luther (2016). The Political Economy of Bitcoin. Economic Inquiry, 54(2), 925-939.

Hileman, G. (2015). The Bitcoin Market Potential Index. In International Conference on Financial Cryptography and Data Security (pp. 92-93). Springer Berlin Heidelberg.

Kaplanov, N. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. Loy. Consumer L. Rev., 25, 111.

Kirby, P. (2014). Virtually Possible: How to Strengthen Bitcoin Regulation Within the Current Regulatory Framework. NCL Rev., 93, 189.

Lane, J. (2013). Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation. Charleston L. Rev., 8, 511.

Lee Kuo Chuen, D. (2015). Handbook of Digital Currency. *Elsevier*.

Malinova, K. y A. Park (2016). Market Design with Blockchain Technology

Möser, M., R. Böhme y D. Breuker (2014). Towards Risk Scoring of Bitcoin Transactions. In *International Conference on Financial Cryptography and Data Security* (pp. 16-32). Springer, Berlin, Heidelberg

Möser, M., R. Böhme y D. Breuker (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, In *eCrime Researchers Summit (eCRS), 2013* (pp. 1-14). IEEE.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Reyes, C.L. (2016). Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal.

Rogojanu, A. y L. Badea (2014). The Issue of Competing Currencies.

Tsukerman, M. (2015). The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future. Berkeley Tech. LJ, 30, 1127.

Tu, K.V. y M.W. Meredith (2014). Rethinking Virtual Currency Regulation in the Bitcoin Age.

Turpin, J.B. (2014). Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework. Indiana Journal of Global Legal Studies, 21(1), 335-368.

Twomey, P. (2013). Halting a Shift in the Paradigm: The Need for Bitcoin Regulation. Trinity CL Rev., 16, 67.

Yermack, D. (2013). Is Bitcoin a Real Currency? An Economic Appraisal (No. w19747). National Bureau of Economic Research.

Anexos

Anexo 1: Postura de Autoridad Bancaria Europea

La EBA es la institución encargada de la regulación y supervisión del sector bancario a nivel europeo. Esta institución contribuye mediante la elaboración de guías y normativa para el sector bancario con el objetivo de armonizar las normas para las instituciones financieras de la Unión Europea (en adelante UE).

La EBA reconoce la creciente popularidad de estas monedas virtuales y, por ende, advierte a los usuarios que las plataformas de intercambio de dinero real por Bitcoins no están reguladas por una autoridad bancaria y, por tanto, su dinero virtual no será aceptado como un depósito en los bancos tradicionales.

La institución indica que, si bien la información sobre las transacciones en moneda virtual es pública, la identidad de los dueños y destinatarios de estas transacciones no lo es, lo que produce que éstas sean en gran medida imposibles de rastrear, ofreciendo así un alto grado de anonimato a los usuarios de divisas virtuales.

Así también, la EBA advierte sobre las posibles obligaciones tributarias originadas a partir del uso de Bitcoin. La entidad señala que la posesión de monedas virtuales puede tener implicaciones impositivas, como el IVA o el impuesto sobre las ganancias de capital.

En su informe de julio de 2014, la EBA señala los beneficios y riesgos del uso de monedas virtuales, los cuales se resumen a continuación:

Beneficios

Menores costos de transacción: Debido a la ausencia de intermediarios, las monedas virtuales permiten incurrir en menores costos que otros medios de pago tradicionales como las tarjetas de crédito o las transferencias bancarias. De acuerdo con el informe, esto se debería en parte a la ausencia de requerimientos en términos regulatorios que hay actualmente aplicados a este tipo de transacciones.

Menor tiempo en procesar transacciones: Las transacciones mediante Bitcoin apenas tardan entre 10 y 60 minutos en realizarse y confirmarse, muy por debajo de las transacciones realizadas mediante otros medios de pago. Esta diferencia es especialmente notable cuando se trata de transacciones entre diferentes países.

Certeza del recibo de los pagos: Uno de los problemas que sufren los comerciantes que emplean otros medios de pago, son las reversiones de los pagos basadas en falsas reclamaciones. En el caso de Bitcoin, una vez confirmado un pago, se vuelve prácticamente imposible revertirlo, lo que se convierte en un beneficio para el vendedor.

Mayor inclusión financiera fuera de la UE: En países donde se cuenta con un sector económico débil y una moneda poco estable, Bitcoin proporciona acceso a servicios financieros sin discriminación ni costo, con tan sólo tener un teléfono móvil con acceso a la red.

Beneficios individuales: Consisten principalmente en la seguridad de los datos personales y la no interferencia de las autoridades públicas. Bitcoin proporciona la libertad y privacidad necesarias a aquellas personas que han dejado de confiar en los sistemas financieros tradicionales.

Riesgos

La EBA, junto con el Banco Central Europeo y la Autoridad Europea del Mercado de Valores han identificado cerca de 70 riesgos asociados a las monedas virtuales. Muchos de estos riesgos tienen que ver con el hecho de que las plataformas de las monedas virtuales son abiertas y pueden ser modificadas de manera anónima por quienes tengan las suficientes capacidades informáticas.

A grandes rasgos, estos riesgos podrían resumirse en robo de identidad, pérdida del dinero de los usuarios por fraude o ataque de *hackers* a la plataforma de operaciones, volatilidad en el precio, cambios en la normativa aplicable, incumplimientos de las leyes, dificultad en convertir las monedas virtuales en monedas convencionales, pérdida del acceso a sus fondos y facilidad para su uso en actividades delictivas.

Adicionalmente, se presenta una serie de riesgos para las autoridades reguladoras:

Riesgos de pérdida de reputación: Si se diese el caso de que las instituciones financieras comenzaran a utilizar monedas virtuales sin haber sido antes reguladas, complicaría la regulación actualmente aplicable a estas instituciones. También podría darse el caso de intentar regular las monedas virtuales y equivocarse en el análisis.

Riesgos legales: Una vez que las autoridades reguladoras decidan comenzar a regular las monedas virtuales, un error en el análisis podría provocar que las actividades de algunos participantes actuales en el mercado se vuelvan ilegales.

Riesgos para la libre competencia: Regular de forma diferente las mismas actividades que ya se llevan a cabo en el mercado, pero en que se usan monedas virtuales, crearía un terreno desigual en el mercado.

Por todo lo expuesto, la EBA recomendó a los bancos europeos no comprar, poseer ni vender monedas virtuales hasta que los organismos reguladores desarrollen formas de proteger su integridad[18].

Propuesta de regulación

Para mitigar los riesgos enumerados, la EBA propuso una serie de medidas regulatorias aplicables a las monedas virtuales. La mayoría de las medidas son conocidas y ya se aplican a muchas de las empresas que operan con monedas virtuales, intentando que estas empresas cumplan con las leyes a las que se someten las entidades financieras tradicionales.

Sin embargo, existe un punto especialmente controversial debido a la falta de viabilidad de su aplicación en Bitcoin: Para hacer frente a los riesgos derivados de que cualquier persona (incluyendo criminales) pueda crear de forma anónima una moneda virtual sin hacerse responsable de ningún posible perjuicio a terceros, sería necesaria la creación de una entidad responsable ante

[18] Las advertencias de la EBA contrastan con el reciente informe del *Bank of America Merrill Lynch* que considera al Bitcoin como una alternativa en aquellos países inestables, con control de capitales o con moneda muy intervenida.

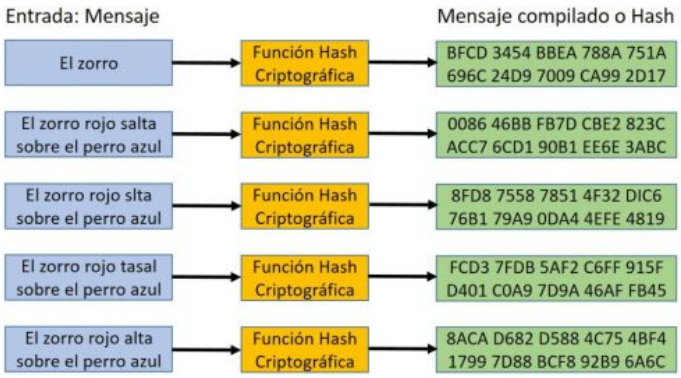
el regulador como requisito para que una moneda virtual sea regulada como servicio financiero y por lo tanto para que se le permita operar con los sistemas regulatorios existentes. Esta entidad sería la responsable del correcto funcionamiento de la moneda virtual, lo que sería completamente incompatible con el actual funcionamiento descentralizado de Bitcoin y las demás monedas virtuales.

Anexo 2: Función *hash* criptográfico en Bitcoin

Una función criptográfica *hash*, usualmente conocida solo como "*hash*", es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independiente de la longitud de los datos de entrada, el valor *hash* de salida tendrá siempre la misma longitud.

En otras palabras, una función *hash* es cualquier función que puede ser usada para mapear data de un tamaño arbitrario a data de tamaño fijo en una cantidad de tiempo razonable. Los valores generados por una función *hash* son llamados valores *hash*, códigos *hash* o simplemente *hash*. En la Figura N° 11 se ilustra el mapeo de datos que realiza la función *hash*.

Figura N° 11: Función *hash*



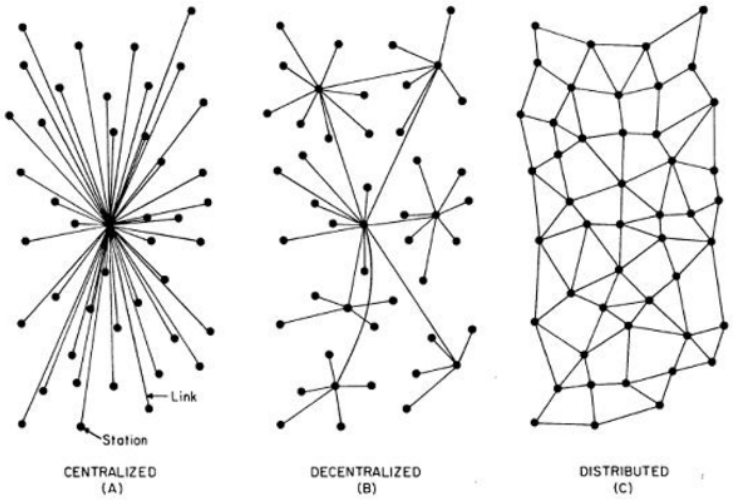
La función hash criptográfica en ejecución. Un pequeño cambio en la entrada (en la palabra "salta") cambia drásticamente la salida. Esto se conoce como efecto avalancha. Fuente: Wikipedia.

En el caso de Bitcoin, la información contenida en cada bloque es registrada en forma de *hash* criptográfico, lo que permite su fácil verificación, pero hace inviable recrear la data de entrada. Particularmente, Bitcoin usa la función *hash* criptográfica SHA-256 lo que implica que sus apuntadores *hash* son de un tamaño fijo de 256 *bits*.

Anexo 3: *Blockchain* es una red distribuida, no descentralizada

La cadena de bloques o el sistema *blockchain* es una red P2P en la que todos los nodos son iguales entre sí dando como resultado un sistema distribuido resistente a ataques informáticos, fallas o falsificaciones. De esta manera, aunque un nodo fallase se podría llegar a aquellos otros a los que está conectado por vías alternativas. Esto no sería posible en un sistema descentralizado.

Figura N° 12: Ilustración de diferencias entre diferentes tipos de estructuras

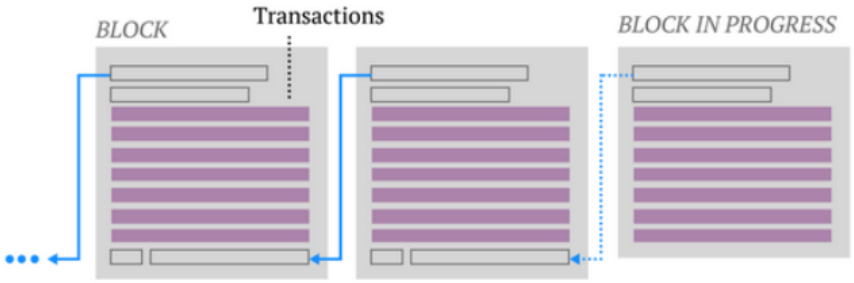


Anexo 4: Qué es un bloque

Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques. Cada bloque que forma parte de la cadena (excepto el bloque generatriz, que dio inicio a la cadena) está formado por:

1. Un código alfanumérico que enlaza con el bloque anterior.
2. El paquete de transacciones que incluye (cuyo número viene determinado por diferentes factores).
3. Otro código alfanumérico que enlazará con el siguiente bloque.

Figura N° 13: Enlace entre los bloques de información de la cadena a través de códigos alfanuméricos



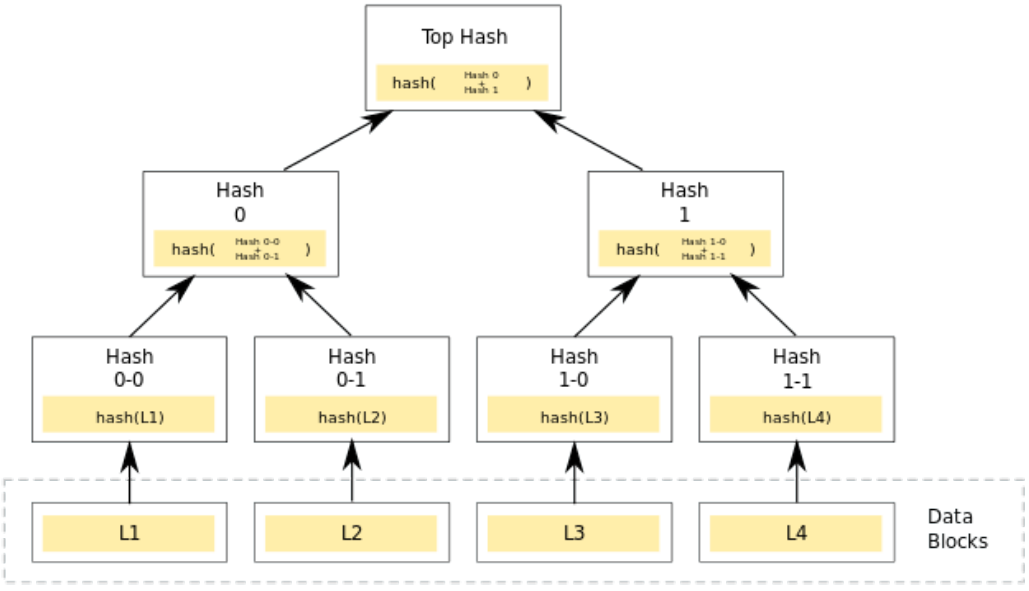
El bloque en progreso intenta averiguar con cálculos e iteraciones numéricas el código que enlazará con el siguiente bloque. Este código sigue determinadas reglas para ser válido y sólo se puede obtener probando sin parar por medio de la capacidad computacional.

Anexo 5: Función Árbol de Merkle

Las transacciones o data se registran en cada bloque de la cadena de bloques en una estructura criptográfica de apuntadores *hash* llamada Árbol de Merkle, debido a su creador Ralph Merkle. Esta estructura agrupa los bloques de información en pares y genera un *hash* por cada bloque de datos. Luego, los *hashes* generados vuelven a ser agrupados en pares y generan un nuevo hash que a su vez se agrupa con otro y se repite camino arriba del árbol hasta alcanzar un único bloque, la raíz del árbol, que se denomina apuntador *hash* raíz (*root hash*) y se registra en la dirección del bloque actual (*block hash*) con el fin de reducir el espacio ocupado por cada bloque.

Además, esta estructura de apuntadores *hash* permite recorrer cualquier punto del árbol para verificar que los datos no han sido manipulados, ya que, al igual que con la cadena de bloques, si alguien manipula algún bloque de datos en la parte inferior del árbol, hará que el apuntador *hash* que está un nivel más arriba no coincida, e incluso, si continúa manipulando este bloque, el cambio eventualmente se propagará a la parte superior del árbol en la que no será capaz de manipular el apuntador *hash* que hemos almacenado por pertenecer a otra estructura (cadena de bloques) en la que también se ha generado un *hash* utilizando el *hash* raíz como entrada. Así que, de nuevo, se detectará cualquier intento de manipular cualquier pieza de datos con sólo registrar el apuntador *hash* en la parte superior.

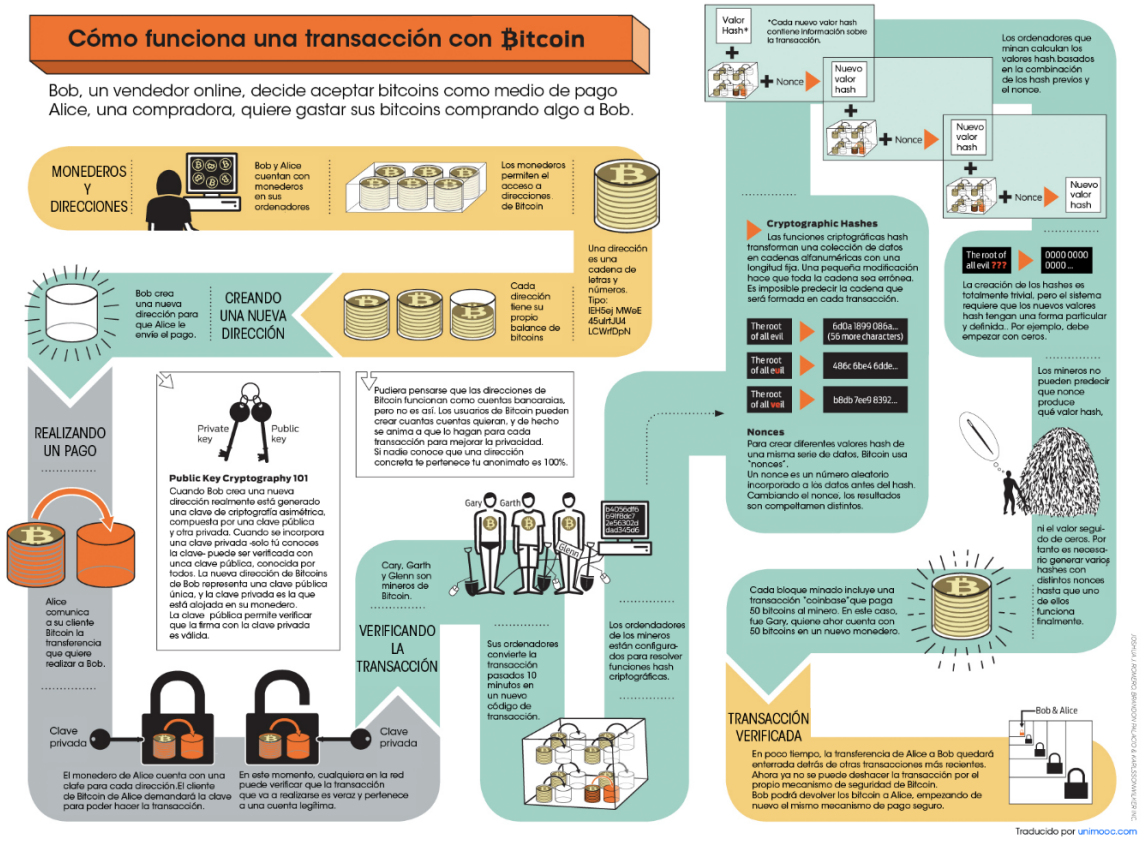
Figura N° 14: Estructura de Árbol de Merkle



Fuente: Wikipedia

Anexo 6

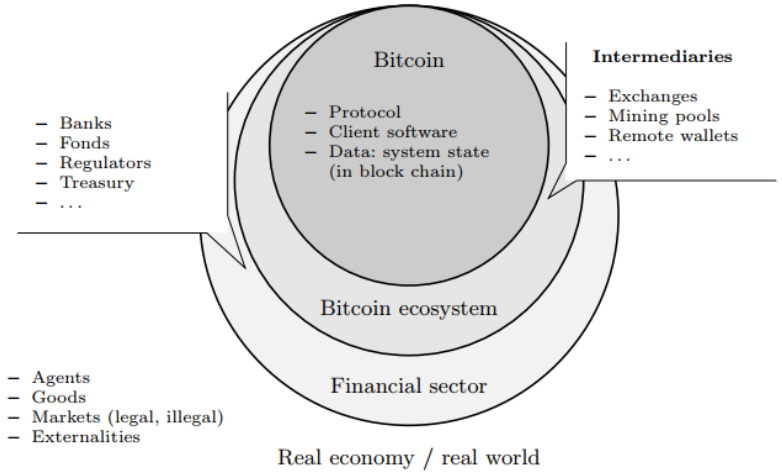
Figura N° 15: Cómo opera la tecnología *blockchain* en una transacción con Bitcoin



Fuente: Infografía originalmente publicada en inglés en spectrum.ieee.org, y traducida al español por UniMOOC.com

Anexo 7

Figura N° 16: Relación de sistema Bitcoin con el mundo real



Fuente: Möser et al. (2014)