I.
QUÉ ES BITCOIN Y CÓMO FUNCIONA

Un camino no recorrido

Si bien la moneda nació como una institución liberadora y promotora de la cooperación entre los seres humanos, con el tiempo los gobiernos han logrado convertirla en una herramienta de control social cada vez más sofisticada. Es por eso que todos los emprendedores involucrados en la creación de monedas de uso voluntario –es decir, no impuestas por la fuerza– se han tenido que enfrentar al largo brazo de la ley (bien armado, por cierto).

Entre el tendal de víctimas podemos encontrar al *Liberty Dólar* y a su creador, Bernard von NotHaus, quien sufriera una redada por parte del FBI en la que se confiscaron todos sus activos (el oro y la plata que respaldaban dicha moneda), y quien fuera luego condenado a prisión. Otros casos conocidos son los de *eGold* (compañía que solía permitir la transferencia de letras digitales con respaldo en oro, también arruinada por el gobierno de los EE.UU.) y *Goldmoney* (compañía que aún resiste el acoso del gobierno de los EE.UU., y que ha sido obligada a cancelar su servicio en varios países, y a cancelar su sistema de pagos en línea en todas partes).

Pero Bitcoin ha llegado para cambiar las reglas del juego. Este increíble ejemplo de ingenio y visión reúne todas las cualidades deseables en un medio de intercambio indirecto (dinero), y está libre de aquellos problemas que a menudo limitan las ventajas de tan importante herramienta, a saber: elevados costes de traslado y transacción, exposición a violaciones de la seguridad y la privacidad, posibilidad de expansión crediticia con fines políticos (causa principal del ciclo económico) e

inflación (pérdida del poder adquisitivo) por aumento discrecional de la masa monetaria, entre otras muchas distorsiones derivadas de la intervención gubernamental. Veamos en detalle de qué se trata…

Generalidades

Bitcoin es una *moneda electrónica* descentralizada, concebida en 2009 por quien se ha dado a conocer como Satoshi Nakamoto (aunque su verdadera identidad se desconoce). El nombre Bitcoin se aplica también al *software libre* diseñado por Nakamoto para la gestión de dicha moneda, y a la red *P2P* (*peer to peer*, o red de «pares» bajo un mismo protocolo) que le da soporte. A diferencia de la mayoría de las monedas, el funcionamiento de Bitcoin no depende de una institución central, sino de una *base de datos distribuida*. El software ideado por Nakamoto emplea la *criptografía* para proveer funciones de seguridad básicas, tales como la garantía de que los bitcoins solo puedan ser gastados por su dueño, y nunca más de una vez.

Bitcoin es una de las primeras funciones prácticas del concepto de *criptomoneda*, y sin duda la más exitosa hasta la fecha. La propuesta que inspiró a Nakamoto –de una forma de dinero electrónico imposible de monopolizar, irrastreable y que les permite a sus dueños mantenerse anónimos– fue descrita por primera vez en 1998 por el criptógrafo Wei Dai en la célebre lista de correo electrónico Cypherpunk. El diseño de Bitcoin, de hecho, permite poseer y transferir valor entre cuentas públicas de forma potencialmente anónima.

Quizás el mayor logro de Satoshi Nakamoto sea el de haber resuelto el problema del doble gasto en un sistema descentralizado, que tanto ha desvelado a economistas y programadores. Para evitar que un mismo bitcoin sea gastado más de una vez por la misma persona (en otras palabras, para evitar la falsificación), la red se vale de lo que Nakamoto describe como un *servidor de tiempo distribuido*, que identifica y ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de *pruebas de trabajo* encadenadas (las cuales

se muestran como «confirmaciones»). Más adelante veremos que dicho trabajo es realizado por los «mineros de bitcoins» a cambio de una recompensa en bitcoins.

Si bien el envío de bitcoins es instantáneo, y cualquier operación puede ser monitoreada en tiempo real, las confirmaciones que nos muestra la pantalla cuando usamos el software de Bitcoin vienen a representar el proceso de *clearing*. A mayor número de confirmaciones, más remota será la posibilidad de ser víctima de un doble gasto. Cuando supera las cinco confirmaciones por parte de la red, una transacción es considerada técnicamente irreversible.

Seguridad

Cabe destacar que, hasta la fecha, no se ha documentado ningún caso de doble gasto, pero es cierto que un ataque informático de este tipo es teóricamente posible, siempre y cuando el atacante controle al menos el 51% del poder computacional que protege a la red. Sin embargo, engañar a la red el tiempo suficiente como para llevar a cabo un único doble gasto implicaría una inversión tan descomunal (el poder de cómputo de la red Bitcoin es varias veces superior al de las 100 supercomputadoras más rápidas que existen, todas combinadas), y una organización tan compleja que desde un punto de vista económico sería infinitamente más provechoso poner esos recursos a trabajar bajo las reglas del protocolo Bitcoin. Por otra parte, el código ha sido recientemente modificado para facilitar la detección y neutralización de este tipo de ataques –sean cuales sean sus motivaciones–.

La inmensa mayoría de los que aceptan bitcoins se conforman con una única confirmación. Para montos pequeños es razonable, incluso, aceptar transacciones instantáneamente –antes de que sean confirmadas por la red–.

La información que habilita el control de los bitcoins que uno posee puede ser guardada en cualquier soporte de información digital (disco rígido personal, tarjeta o llave de memoria, CD, casilla

de web-mail, etc.) en la forma de un archivo «billetera», o bien custodiada por sitios web que ofrecen «cuentas Bitcoin». También es posible mantener dicha información en soportes no digitales (impresa en papel, por ejemplo) y hasta en el propio cerebro. La posesión de los bitcoins puede ser transferida por medio de internet a cualquiera que tenga una «dirección Bitcoin», a semejanza de la manera en que se envía un e-mail a una dirección de correo electrónico.

Según los expertos, gracias a la arquitectura criptográfica de Bitcoin una transferencia entre direcciones Bitcoin es varias veces más segura que una transferencia entre cuentas bancarias (sin contar el riesgo que implica la forzosa intromisión de terceros en el sistema bancario).

En resumen

Puede decirse que Bitcoin funciona como un libro contable descentralizado, en el cual los saldos no están ligados a los usuarios sino a las direcciones públicas que ellos controlan. El historial de todos los movimientos de bitcoins permanece almacenado en la cadena de bloques, una base de datos distribuida que mantiene el registro de todas las transacciones en cada uno de los múltiples nodos que integran la red (ver más adelante «Cadena de bloques»). Estos nodos no son más que computadoras ejecutando el software de Bitcoin en todo el mundo, conectadas entre sí por medio de internet.

La naturaleza P2P de la red Bitcoin hace imposible el establecimiento de un control centralizado de todo el sistema. Esto impide el aumento arbitrario de la cantidad de bitcoins en circulación (lo que generaría *inflación*) y cualquier otro tipo de manipulación del valor por parte de las autoridades.

Información técnica

Los principios del sistema están detallados en el *Paper de Bitcoin*, escrito en el año 2008 por Satoshi Nakamoto.

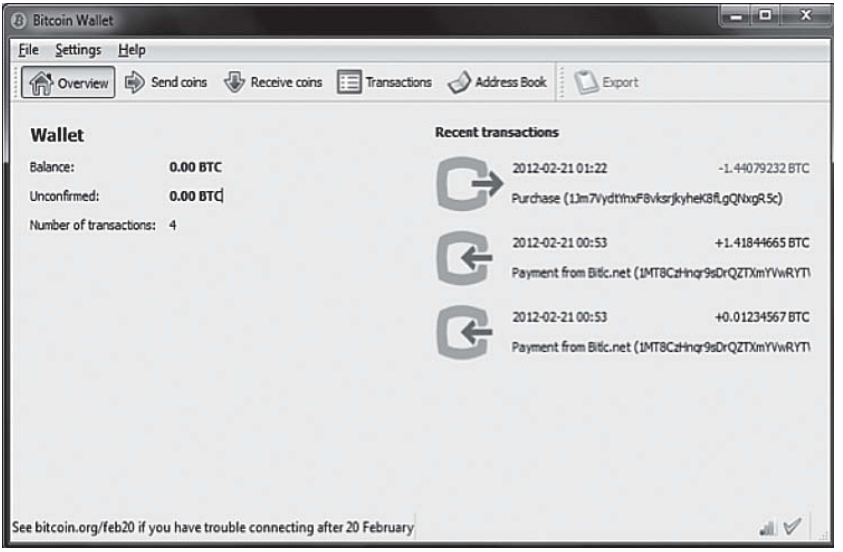
Direcciones

Cualquier persona que participa en la red Bitcoin posee una billetera electrónica que contiene pares de llaves criptográficas. Las *direcciones* Bitcoin visibles derivan de las llaves públicas de cada usuario, y a su vez funcionan como los puntos *remitente/receptor* para todos los pagos. Las llaves privadas correspondientes a cada llave pública sirven para que un determinado usuario autorice pagos (transfiera bitcoins) desde su billetera.

Las direcciones públicas no tienen ninguna información sobre sus dueños; estas aparecen como secuencias aleatorias de números y letras de 33 caracteres de largo, como por ejemplo:

1rYK1YzEGa59pI314159KUF2Za4jAYYTd

Los usuarios de Bitcoin pueden tener múltiples direcciones; de hecho, pueden generar direcciones nuevas fácilmente y sin límites.



Bitcoin-Qt: Software de Bitcoin.

Generar una nueva dirección equivale a generar un nuevo par de llaves (pública/privada), y no requiere ningún contacto con nodos de la red. Los usuarios que desean preservar el anonimato suelen crear una nueva dirección para cada transacción.

Transacciones

Cuando un usuario ***A*** transfiere bitcoins a un usuario ***B***, el usuario ***A*** renuncia a su posesión de un determinado número de bitcoins, agregándoles la llave pública de ***B*** y firmando la combinación resultante con su llave privada. (Gracias al empleo de la criptografía asimétrica, la llave privada no puede ser deducida de la firma que de ella deriva.) Esta información se transmite a toda la red *P2P* como una nueva *transacción*. Entonces, el resto de los nodos de la red verifican el número de bitcoins involucrados y la autenticidad de las firmas criptográficas, antes de aceptar la transacción como válida.

Cadena de bloques

Cualquier transacción transmitida a otros nodos no se convierte inmediatamente en «oficial»; primero tiene que ser confirmada en una lista –mantenida colectivamente– de todas las transacciones conocidas: la *cadena de bloques*. Tal es el trabajo de los *nodos generadores*, cuyos dueños son los *mineros de bitcoins*.

Cada nodo generador de bitcoins recoge todas las transacciones que aún no fueron confirmadas en un archivo (el bloque candidato) que contiene la referencia a dichas transacciones y al último bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un *hash* de ese bloque (un código aleatorio que lo representa), en un esfuerzo computacional que demanda cantidades predecibles de intento y error. Cuando un nodo encuentra la solución, la transmite a toda la red. El resto de

los nodos reciben el nuevo bloque solucionado, lo verifican antes de aceptarlo y lo agregan a la cadena.

Aunque ningún usuario de Bitcoin está forzado a revelar su identidad, todas las transacciones jamás realizadas quedan grabadas en esa base de datos de libre acceso que es la cadena de bloques. Esta contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de Bitcoin. Por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó (doble gasto), la red lo detectará y rechazará la transacción.

La cadena de bloques es un registro totalmente transparente: cualquiera puede examinarla, en cualquier momento, para informarse acerca de cualquier transacción que se haya realizado desde el lanzamiento de Bitcoin, así como de las nuevas transacciones que se van agregando a la cadena en tiempo real. Varios servicios facilitan este tipo de monitoreo.

Cómo se generan los bitcoins

Aproximadamente seis veces por hora, la red Bitcoin crea y distribuye un lote de nuevos bitcoins a quien esté ejecutando el software para generar bitcoins (*software* de «minería»). Generar bitcoins es conocido como «minar», un término que remite a la minería de metales preciosos. La probabilidad de que un usuario reciba un lote depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados.

El primer nodo generador en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de bitcoins. Los «mineros» también pueden unirse por medio de internet para generar bitcoins en grupo, formando un *pool* minero.

La cantidad de bitcoins creada por lote nunca es ni será mayor a 50 BTC, y los premios (el número de bitcoins por lote) están programados para disminuir con el paso del tiempo, reduciendo el incremento de la masa monetaria de manera predecible, hasta llegar a cero. Nunca llegarán a existir más de 21 millones de bitcoins.

Para que un bloque sea generado cada diez minutos, el protocolo actualiza cada dos semanas la dificultad del problema que todos los nodos generadores están intentando resolver, ajustándola al poder computacional de toda la red.

Debido a los incrementos en la dificultad para obtener bitcoins por medio de la minería, ya hace mucho tiempo que esta dejó de estar al alcance del usuario común de un PC. Hoy en día, la mayoría de los usuarios de Bitcoin obtienen sus cripto-monedas a cambio de los productos que venden, o en sitios de *trading*, o bien en transacciones cara a cara con mineros u operadores que compran bitcoins y los venden cobrando una comisión.

Tarifa de transacción

Debido a que los nodos no tienen la obligación de incluir transacciones en los bloques que generan, los remitentes de bitcoins pueden pagar voluntariamente una tarifa de transacción. Al hacerlo, además de acelerar la transacción, proveen incentivos a los usuarios que mantienen nodos generadores (vale decir, a los mineros). Los nodos generadores retienen el valor correspondiente a las tarifas de todas las transacciones incluidas en los bloques que han resuelto.

Dichas tarifas –cuando se pagan– suelen ser una fracción insignificante del monto enviado, si se las compara con las de cualquier otro sistema de transferencia de valor. Por ejemplo, si decidimos enviar 100 bitcoins puede que el software nos sugiera pagar una tarifa de 0,005 bitcoins.

Las tarifas de transacción irán cobrando más importancia cuanto más bajo sea el premio por bloque. En el futuro, los mineros se

verán motivados a mantener los nodos generadores por la suma de pagos en concepto de tarifas que puedan acumular, más que por los bitcoins que sean capaces de generar.

Peculiaridades monetarias

A diferencia del *dinero de curso forzoso*, Bitcoin no puede ser controlado por ninguna autoridad debido a su naturaleza descentralizada. La expansión de la base monetaria está predeterminada por el software de Bitcoin y es conocida por todos, de modo que no es posible afectar el poder adquisitivo de los usuarios manipulando la cantidad de bitcoins en circulación.

Bitcoin es un medio de pago irreversible. Las transferencias son realizadas directamente entre los nodos, sin un procesamiento centralizado por un tercero, lo cual hace imposible tanto la reversión involuntaria de pagos como la cancelación de transacciones mutuamente acordadas.

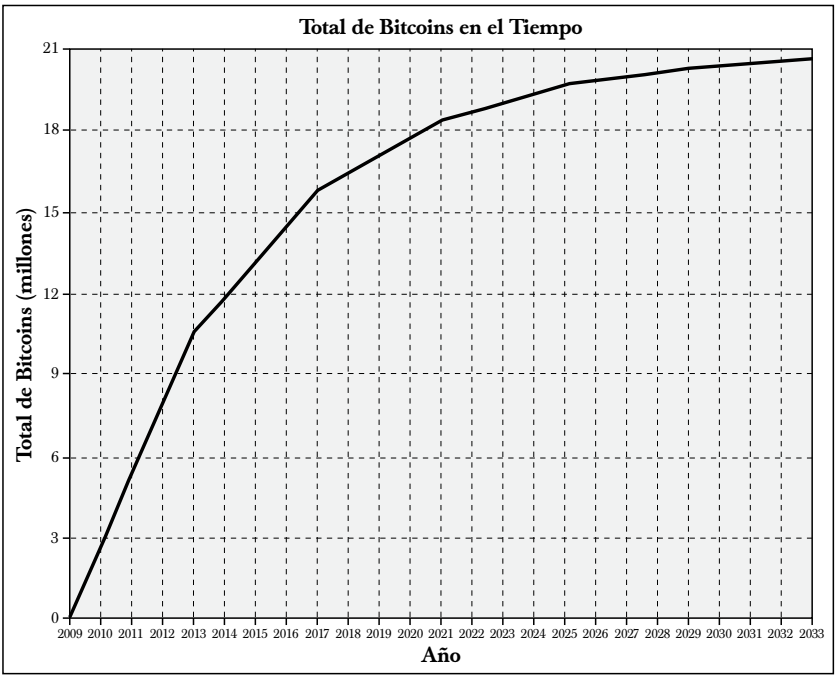
Así, el envío de bitcoins se asemeja, en los beneficios y en los riesgos que supone, al envío de dinero en efectivo. No obstante, muchos sitios ofrecen servicios similares a *eBay* o *Mercado Libre* para facilitar el intercambio de bienes y servicios por bitcoins (por ejemplo, promoviendo la calificación entre los usuarios y/o reteniendo los fondos hasta que las partes expresan conformidad).

El software de Bitcoin (también denominado «cliente Bitcoin») que los usuarios tienen instalado en sus ordenadores transmite cada transacción a los nodos cercanos, que a su vez la propagan a toda la red. Las transacciones inválidas son rechazadas por los clientes honestos (aquellos que se atienen al protocolo de la cadena de bloques en uso). Por el momento, la mayoría de las transacciones pueden realizarse gratuitamente, pero ya hemos visto que es posible pagar una tarifa para que los mineros prioricen (aceleren) su procesamiento.

El número total de bitcoins tenderá a 21 millones con el tiempo. Su oferta crece en una serie geométrica (con una razón constante);

así, en 2013 la mitad de la oferta total habrá sido generada, y en 2017, 3/4 de esta. A medida que la cantidad de bitcoins se aproxime al límite de 21 millones, se espera que la economía Bitcoin entre en *deflación*, esto es, que el poder adquisitivo de cada bitcoin aumente, probablemente hasta alcanzar cierta estabilidad.

Los bitcoins, entre tanto, son divisibles hasta ocho decimales (dándonos 2,1 x 10^{15} –vale decir 2,1 cuatrillones– de unidades totales), y potencialmente aún más de ocho decimales, lo cual remueve las limitaciones prácticas a los ajustes de precio en un contexto deflacionario.



La economía Bitcoin es aún pequeña si la comparamos con otras economías ya establecidas, y el *software* todavía se encuentra en estado *beta*. Sin embargo, todo tipo de bienes y servicios, desde automóviles a trabajos de programación *freelance*, están en este momento siendo intercambiados por bitcoins. Además, hay *gran cantidad de sitios*

web que facilitan el intercambio de todo tipo de divisas por bitcoins, y admiten diversos sistemas para transferir los fondos.

¿En qué resultará?

Un posible escenario de fracaso para Bitcoin es el de una campaña gubernamental global en contra del software y de los sitios que aceptan bitcoins. Pero, dada la naturaleza del sistema, la eliminación total de Bitcoin (así como de cualquier otra red P2P) no parece tecnológica ni económicamente viable.

Nadie sabe con certeza cuál será el destino de Bitcoin; todo lo que sabemos es que la idea de una cripto-moneda descentralizada llegó para quedarse.

Por qué nos cuesta entender el funcionamiento de Bitcoin

Incluso los más preparados entre nosotros parecen requerir al menos dos o tres explicaciones antes de comprender efectivamente cómo es que funciona Bitcoin. Esto se debe a que *Bitcoin desafía una serie de conceptos rara vez cuestionados*, de los que es necesario desprenderse si se han de incorporar otros mejores.

El esfuerzo, por lo tanto, es doble. Así como la teoría de la universalidad de los «cuatro elementos» (aire, agua, fuego, tierra) entorpeció durante siglos el progreso científico, la teoría cuantitativa del dinero –y su correlato de un sistema monetario dirigido por «especialistas», con un banco de bancos en su centro– ha tenido un efecto mental devastador sobre generaciones enteras de legos y estudiosos.

El problema es que, aun sabiendo por qué Bitcoin es superior a cualquier otro sistema monetario, muchos tienden a preferir lo ya conocido con tal de no incursionar en territorios inexplorados. La eterna batalla entre el conservador –partidario de lo malo conocido– y el aventurero –partidario de lo bueno por conocer– se libra en

realidad en el pecho de cada ser humano. Pero, una vez rechazado el legado de ideas falsas y *vencida la inercia de las costumbres, el camino se hace cuesta abajo* para el aventurero –quien abrirá paso también al conservador–.

¿Cuáles son esas costumbres tan arraigadas que hacen aparecer a Bitcoin como algo inverosímil?

- **Estamos habituados a que el acto de pagar esté separado del acto de registrar el pago.** En rigor, por medio de Bitcoin nadie paga (nadie envía ni recibe bitcoins). Lo que hace la gente es modificar saldos en una suerte de libro contable descentralizado. Así pues, el acto de pagar se confunde con el de registrar el pago.
- **Estamos habituados a pensar que el sistema monetario necesita ser custodiado por una casta privilegiada.** El protocolo de Bitcoin no protege a alguien o a algún grupo en particular, sino a la herramienta misma – y así a todos los que la usan.
- **Estamos habituados a que nuestras cuentas bancarias estén asociadas a nuestra identidad.** Las direcciones Bitcoin son anónimas si así lo desean sus dueños.
- **Estamos habituados a que el movimiento de fondos sea conocido solo por quienes están directamente involucrados en una transacción (las partes y el tercero que procesa el pago).** En Bitcoin la información acerca de todas las transacciones es pública y de fácil acceso.
- **Estamos habituados al dinero como recibo con más o menos respaldo.** En el caso de Bitcoin, unidad y recibo son una misma «cosa» imposible de replicar o falsificar.