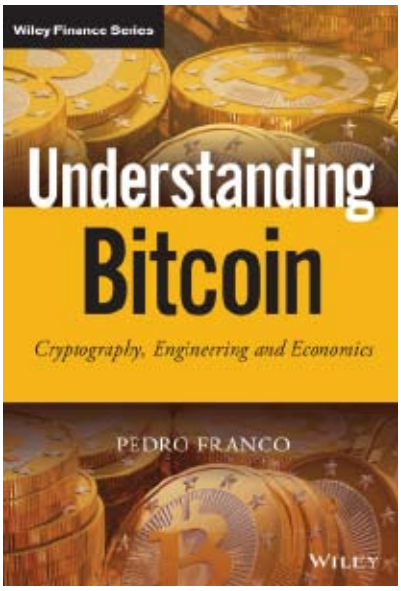


Entendiendo Bitcoin: Criptografía, Ingeniería y Economía

A continuación se reproduce el capítulo "Las bases de Bitcoin", extraído del libro "Entendiendo Bitcoin: Criptografía, Ingeniería y Economía" del original en inglés "Understanding Bitcoin: Cryptography, Engineering and Economics", editado por John Wiley & Sons en 2014 y cuyo autor es Pedro Franco.

Las bases de Bitcoin

Ha habido una amplia cobertura en los medios de comunicación acerca de Bitcoin, y muchas figuras públicas se han visto obligadas a expresar su opinión. Como Bitcoin es un tema complejo, que cubre criptografía, ingeniería de *software* y economía, es difícil captar su esencia y las implicaciones de este fenómeno tras sólo un estudio superficial. En consecuencia, muchas de estas figuras públicas podrían no tener una idea clara de cómo funciona y cuáles son sus implicaciones. El objetivo de este libro es dotar al lector de los conocimientos necesarios para evaluar las características de esta tecnología.

La Figura 1 resume algunos conceptos erróneos alrededor de Bitcoin.

Bitcoin es una moneda digital descentralizada. Esto quiere decir que no hay ninguna persona o institución detrás de ella, ya sea respaldándola o controlándola. Bitcoin tampoco está respaldada por ningún bien físico, como los metales preciosos. Esto puede parecer contraintiuitivo a primera vista: ¿cómo puede existir una moneda que nadie controla?, ¿quién la creó entonces?, ¿cómo es que el creador ha perdido el control sobre ella?

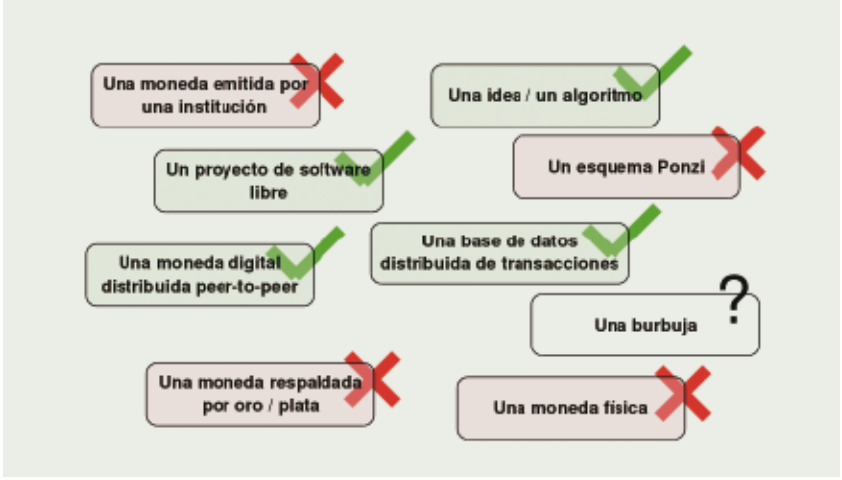
La respuesta a esta aparente paradoja es que Bitcoin es sólo un programa de ordenador. Cómo funciona exactamente este programa es el foco de la segunda parte de este libro. El programa cuenta con un creador (o creadores), pero se desconoce su identidad real ya que su creador utilizó lo que se cree que es un seudónimo: Satoshi Nakamoto. Bitcoin no es controlado en el sentido estricto por una persona. Su creador no perdió el control porque él (ella?, ellos?) nunca tuvo la propiedad del código. El código es **código libre** y por lo tanto pertenece al dominio público, como se explicará con más detalle en la sección 1.2.

Una de las características más innovadoras de Bitcoin es que es **descentralizado**. No hay un servidor central donde se esté ejecutando Bitcoin. Bitcoin opera a través de una red de ordenadores conectados par-a-par *(peer-to-peer)*. Bitcoin es la primera moneda digital descentralizada y, en este sentido, constituye un gran avan-

Pedro Franco

Ingeniero Industrial Eléctrico por el ICAI. Ha sido consultor en McKinsey y Boston Consulting Group e investigador del IIT. Los últimos 10 años ha centrado su labor profesional en los mercados financieros en posiciones de Quant y Trader en crédito, riesgo de contraparte, inflación y tipo de interés. Ha creado varias librerías matemáticas para la valoración y gestión de derivados financieros, y ha gestionado equipos de desarrolladores de *software*. Es autor del libro "Understanding Bitcoin: cryptography, engineering and economics", John Wiley & Sons, 2014.

Figure 1. Qué es (y qué no es) Bitcoin



ce tecnológico. La naturaleza descentralizada de Bitcoin se explorará con más detalle en la sección 1.1.

El sistema Bitcoin crea su propia moneda llamada bitcoin, con b minúscula. La creación de una moneda es una parte integral del funcionamiento del sistema, ya que tiene dos objetivos simultáneos. En primer lugar, sirve para representar el valor. En segundo lugar, la emisión de nuevas bitcoins se utiliza para recompensar a los operadores de la red que aseguran con su potencial computacional la base de datos distribuida. Estas dos funciones no pueden ser desagregadas sin cambiar significativamente el diseño.

El corazón de la red Bitcoin es una base de datos que registra las transacciones que han tenido lugar en el pasado. De esta base de datos es fácil deducir a quién pertenecen los fondos en el instante actual. Esta base de datos a veces se compara con un libro contable cuyas entradas representan a los propietarios de los fondos. Bitcoin no es la primera base de datos distribuida que ha sido creada. Sin embargo, los requisitos de una base de datos financiera son diferentes de los de otras aplicaciones, tales como el intercambio de archivos o los sistemas de mensajes o chat. En particular, las bases de datos financieras deben estar protegidas contra posibles ataques de usuarios que intentan gastar dos veces sus propios fondos. Este es el problema que Bitcoin resuelve con elegancia y será analizado en las siguientes secciones y en el capítulo 2.

Algunos críticos han argumentado que Bitcoin es un **esquema Ponzi. No lo es**. En un esquema Ponzi hay un operador central que paga rendimientos a los inversionistas actuales utilizando nuevas entradas de capital para ello. En primer lugar, en Bitcoin no hay un operador central que pueda beneficiarse de la reubicación de fondos. En segundo lugar, no existe un mecanismo para desviar fondos de nuevas inversiones para pagar las devoluciones y rendimientos de los participantes actuales. Los únicos fondos reconocidos en el protocolo de Bitcoin son bitcoins, la moneda. Las transferencias de bitcoins son iniciadas por los usuarios bajo su propia voluntad: el protocolo no puede desviar fondos de un usuario a otro. En tercer lugar, una nueva inversión en Bitcoin siempre se corresponde con una desinversión. Los inversores que invierten en bitcoins suelen operar a través de un mercado de intercambio donde compran los bitcoins de otro inversor que está vendiendo su participación. Simplemente, no hay nuevos flujos de inversión en bitcoins: la cantidad de moneda soberana que ha sido invertida en bitcoins es exactamente igual que la cantidad que ha sido desinvertida.

Sin embargo, bitcoin, la moneda, sí puede ser una burbuja. El futuro valor de los bitcoins, tanto si aumenta como si desciende incluso tanto que su valor fuese casi nulo, dependerá de si los bitcoins son utilizados para diferentes aplicaciones. Hay varias aplicaciones interesantes para Bitcoin, de las cuales la más sencilla (pero no la única) es convertirse en un medio de cambio y depósito de valor. Es demasiado pronto para saber si alguna de estas aplicaciones tendrá importancia en el futuro. La fiabilidad de Bitcoin como medio de cambio y depósito de valor se analiza en el capítulo 3.

Por último, Bitcoin no es sólo una moneda, sino toda una infraestructura que puede ser utilizada para transferir valor digitalmente, como se tratará en la sección 1.4 y el capítulo 12.

1. Descentralizado

La mayoría de las monedas en uso hoy en día son las monedas fiduciarias, donde la moneda es emitida por un gobierno y la oferta es gestionada por un banco central.

El dinero fiduciario

La mayoría de las monedas actuales (euro, dólar norteamericano) son dinero fiduciario. El dinero fiduciario no tiene valor intrínseco, ya que no está respaldado por nada. El nombre dinero fiduciario se basa en que hay un decreto del gobierno declarando la moneda de curso legal. La aceptación del dinero fiduciario depende de las expectativas de los usuarios y de una convención social. Si se pierde la confianza en una moneda, por lo general debido a una política monetaria irresponsable, el dinero fiduciario puede dejar de ser aceptado. La experiencia ha demostrado que dejar la política monetaria en manos de los gobiernos no es, por lo general, una buena idea: los gobiernos podrían tener un incentivo en aumentar la oferta monetaria para resolver sus problemas financieros a corto plazo. Este comportamiento puede dar lugar a una alta inflación y una pérdida de confianza en la moneda.

La solución convencional es confiar la política monetaria a un banco central semi-independiente. El banco central tiene la tarea de gestionar la política monetaria, por lo general con los objetivos de crecimiento económico, estabilidad de precios y, en algunos casos, la estabilidad del sistema financiero.

Bitcoin se basa en una red de ordenadores que ejecutan el *software* de manera par-a-par *(peer-to-peer)*. Estos equipos son llamados nodos. Los participantes en la red que mantienen estos nodos tienen diferentes razones para ello: obtener ganancias como en el caso de los mineros (capítulo 9), gestionar carteras de nodo completo (capítulo 8), recopilar y estudiar información acerca de la red (capítulo 13) o simplemente como un bien social.

La naturaleza descentralizada de Bitcoin contrasta con la estructura de las monedas fiduciarias, donde los bancos centrales toman decisiones monetarias después de evaluar la evidencia obtenida de la evolución de la economía. En un sistema descentralizado, como Bitcoin, las decisiones discrecionales no son posibles. Los creadores originales del sistema tienen que tomar la mayor parte de las decisiones por adelantado en la fase de diseño de la moneda. Estas decisiones tienen que ser equilibradas cuidadosamente, y deben tener en cuenta los incentivos de los diferentes usuarios. De lo contrario, un sistema descentralizado estaría abocado al fracaso. En Bitcoin la política monetaria sigue una regla simple: la base monetaria a término está fija en alrededor de 21 millones de bitcoins. Los nuevos bitcoins se crean de acuerdo a un calendario establecido y estos bitcoins son entregados a los usuarios que ayudan a proteger la base de datos distribuida con su potencia computacional. Esto sirve al doble propósito de proveer valor a los bitcoins debido a su escasez y de crear incentivos para que los usuarios se conecten a la red y ayuden a la base de datos dsitribuida aportando la potencia de cálculo de sus ordenadores.

El control en un sistema centralizado se concentra normalmente en una institución o un pequeño grupo de personas clave. Así, los cambios en un sistema centralizado son relativamente fáciles de decidir y ejecutar. El control en una red par-a-par *(peer-to-peer)* es más sutil: los cambios en una red par-a-par tienen que ser acordados al menos por la mayoría de los usuarios. Pero incluso contando con una mayoría, si una fuerte minoría no está de acuerdo con un cambio, la implementación de este cambio puede ser técnicamente difícil y la red corre el riesgo de fracturarse.

Una de las ventajas de la descentralización de poder es que los cambios que sean contrarios a los intereses de la mayoría de los usuarios son, en principio, rechazados más fácilmente. Por el contrario, en un sistema centralizado, a veces se toman decisiones contrarias a la mayoría de los participantes, como ocurre cuando se degrada una moneda debido a la emisión excesiva que generalmente conduce a una alta inflación.

Otra característica de los sistemas descentralizados es su capacidad de recuperación. Los sistemas descentralizados son robustos contra los ataques, ya sean llevados a cabo por personas en posición ventajosa o por atacantes externos. Esta característica puede haber sido fundamental para la supervivencia de Bitcoin desde sus comienzos. Varios de los intentos anteriores realizados para crear monedas digitales centralizadas (sección 2.1) fueron desmantelados por los gobiernos. Sin embargo, para desmantelar un sistema descentralizado, todos los usuarios individuales del sistema deben ser paralizados, lo que constituye una tarea mucho más difícil que desmantelar un sistema centralizado. La naturaleza distribuida de Bitcoin hace que sea resistente a la censura, afirman sus partidarios.

La tecnología para transferir digitalmente valor de manera segura (criptográficamente) ha estado disponible muchos años antes de la creación de Bitcoin (capítulo 10). Sin embargo, la transferencia de valor digitalmente siempre había requerido la creación de un ente centralizado en el que los usuarios debían confiar. Bitcoin no sólo no requiere de un ente central para funcionar, sino que además está diseñado para resistir los ataques de los participantes maliciosos en la red distribuida. Mientras estos participantes maliciosos no controlen la mayoría de la red, estos ataques no tendrán éxito (sección 7.5).

El principal avance tecnológico logrado por Bitcoin constituye la resolución del problema del doble gasto en una base de datos financiera distribuida. Un intento de doble gasto se produce cuando un usuario intenta gastar los mismos fondos dos veces. Todos los sistemas financieros deben rechazar estos intentos. Esto es relativamente sencillo en un sistema centralizado: como las transacciones se registran en una base de datos central y futuros intentos de gastos se comprueban contra esta base de datos, estos intentos son rechazados fácilmente. En un sistema descentralizado, cada uno de los participantes en el sistema distribuido tiene una copia de la base de datos. Mantener un estado consistente de esta base de datos es un problema computacional difícil[1]. En el contexto de Bitcoin el problema es cómo la red puede ponerse de acuerdo sobre el estado de la base de datos distribuida cuando los mensajes entre los nodos pueden ser erróneos, ya que podrían ser generados por atacantes tratando de subvertir la base de datos. Bitcoin resuelve este problema de una manera elegante (sección 2.3 y el capítulo 7).

2. Software libre

Bitcoin es ***software* libre**. El *software* libre consiste en poner el código fuente de un programa a disposición de los usuarios, de manera que cualquiera puede utilizarlo, modificarlo y redistribuirlo de forma gratuita. Algunos de los programas de *software* libre más conocidos son los sistemas operativos Linux y Android o el navegador Firefox. Además, una gran parte de la infraestructura de Internet está basada en *software* libre (menos conocido, pero no menos importante). El objetivo del *software* libre es hacer que el desarrollo de *software* siga un proceso similar a la investigación académica: al publicar el código fuente para que cualquiera pueda leerlo y comprobarlo, el *software* libre permite aumentar la calidad del *software*.

(1) Este problema computacional se denomina problema de los generales bizantinos, introducido en [7].

La diferencia entre el *software* libre y el *software* propietario reside fundamentalmente en la licencia de uso. El *software* propietario otorga en su licencia el derecho a utilizar una copia del programa al usuario final. Sin embargo, la propiedad del *software* sigue siendo del creador de dicho *software*. Por el contrario, una licencia de *software* libre otorga al usuario el derecho a usar, copiar, modificar y redistribuir el *software*. Los derechos de autor del *software* siguen perteneciendo a sus creadores, pero éstos transfieren los derechos al usuario, siempre y cuando el usuario cumpla las obligaciones estipuladas en la licencia.

Otra diferencia entre el *software* libre y el propietario es que el *software* propietario suele distribuirse como ejecutables compilados. Esto significa que este *software* es generalmente distribuido en lenguaje máquina. Los usuarios que deseen adquirir conocimiento sobre lo que está haciendo el *software* deben interpretar el código máquina en un costoso proceso de ingeniería inversa ([4]). De todos modos, la mayoría de las licencias propietarias prohíben el uso de estas técnicas de ingeniería inversa. Así, bajo una licencia propietaria no se le permite al usuario entender o buscar el conocimiento de lo que el *software* está haciendo en realidad. Por el contrario, el *software* libre siempre se distribuye acompañado de una copia del código fuente. El usuario que quiera entender lo que está haciendo el *software* puede simplemente leer el código fuente. El *software* libre que implementa algoritmos criptográficos tiene la ventaja de que permite a los usuarios comprobar que el código no contiene vulnerabilidades de seguridad o puertas traseras[2].

Es poco probable que Bitcoin pudiera haber sido distribuido bajo una licencia propietaria. Si Bitcoin hubiera sido distribuido como *software* propietario, su creador podría haber incluido fácilmente funcionalidades que se desviasen de la especificación, por ejemplo,

creando nuevos bitcoins y enviándolos a una dirección controlada por él. La mayoría de los usuarios probablemente no hubieran aceptado un *software* criptográfico financiero descentralizado distribuido como un ejecutable compilado y bajo una licencia propietaria. Es revelador que la mayoría de las monedas criptográficas alternativas que compiten con Bitcoin (capítulo 11, sección 12.7), o bien han sido creadas usando una licencia de *software* libre o su licencia ha sido cambiada a una licencia de *software* libre.

Las licencias de *software* libre conceden al usuario el derecho de usar, copiar, modificar y redistribuir el *software*. Las diferentes licencias pueden imponer diferentes obligaciones a los usuarios. En términos generales, las licencias de *software* libre pertenecen a una de las siguientes dos familias:

• **"Copyleft".** Este tipo de licencias imponen la obligación de distribuir obras derivadas bajo la misma licencia. Si un usuario del *software* hace modificaciones al mismo, está obligado a distribuir el *software* modificado bajo la misma licencia. Esto se conoce como el requisito de compartir. De este modo, las licencias "copyleft" preservan la naturaleza del *software* libre aún tras sufrir modificaciones. Un ejemplo de licencia "copyleft" es la **GNU Public License (GPL).**

• **"Permisiva".** Este tipo de licencias imponen muy pocas restricciones a la redistribución del *software*, por lo general únicamente que el *software* derivado reconozca los creadores del *software* original y conserve su nota de *copyright*. Si un proyecto de *software* propietario incorporase *software* libre bajo una licencia permisiva, este *software* propietario conservaría su naturaleza propietaria, únicamente requiriendo que el *software* propietario incluya una nota con el copyright del *software* libre que incluye. Varias licencias de *software* libre comunmente utilizadas pertenecen a esta familia, como la licencia BSD, la licencia MIT o la licencia Apache. Bitcoin es distribuido bajo la licencia MIT.

El *software* propietario requiere que la empresa creadora del *software* lo mantenga y actualice. Por el contrario, el *software* libre adquiere vida propia tras ser publicado. No importa si el creador original decide dejar de trabajar en un proyecto de *software* libre ya que otros desarrolladores pueden hacerse cargo del proyecto. Por esta razón, no importa quién sea Satoshi

[2] Esto no quiere decir que el código fuente de *software* libre no contenga fallos de seguridad o puertas traseras. De hecho, muchos fallos de seguridad han sido encontrados en proyectos de *software* libre ([6], [9]). Los defensores del *software* libre argumentan que es más difícil incluir errores de seguridad y puertas traseras en los programas de *software* libre porque existe un mayor nivel de escrutinio, y que estos defectos son típicamente descubiertos y reparados antes que en el *software* propietario ([10]).

Nakamoto, o que haya dejado el proyecto Bitcoin. En este sentido, los proyectos de *software* libre son resistentes: aunque algunos desarrolladores sean obligados a dejar de contribuir o decidan dejar de trabajar en un proyecto, otros desarrolladores de todo el mundo pueden tomar el relevo.

Es legítimo crear un nuevo proyecto de *software* libre a partir de una copia de un proyecto original. Este proceso se llama **bifurcar** *(fork)*. La amenaza de una bifurcación puede hacer que los desarrolladores de un proyecto sean honrados, ya que si los desarrolladores de un proyecto de *software* libre intentan introducir cambios que son perjudiciales para los usuarios, cualquier otro desarrollador puede crear una bifurcación, deshacer los cambios indeseados y continuar con el desarrollo del proyecto. En este escenario, lo más probable es que los usuarios utilicen la bifurcación sin las características indeseadas. La amenaza de una bifurcación puede ser vista como un interruptor que impide que desarrolladores de *software* libre tomen decisiones que van en contra de los intereses de sus usuarios. La mayoría de los grandes proyectos de *software* libre raramente son bifurcados[3]. Bitcoin es algo especial a este respecto, ya que ha sido bifurcado muchas veces por desarrolladores que desean probar nuevos conceptos. Esto ha dado lugar a muchas criptomonedas alternativas llamadas *alt-coins* (del inglés *alternative-coins)*. Las monedas alternativas *(alt-coins)* serán tratadas con más detalle en el capítulo 11.

Los defensores del *software* libre argumentan que las compañías de *software* propietario a menudo pierden el incentivo para innovar una vez que un producto ha alcanzado una posición dominante en el mercado. Muchos mercados de *software* se comportan como monopolios naturales, donde un producto capta una gran cuota de mercado. Por lo tanto, la innovación en muchas categorías de *software* es baja, sugieren los defensores del *software* libre. Por el contrario, aunque un producto de *software* libre capte la mayor parte del mercado, esto no provoca el fin de la innovación, ya que cualquiera puede seguir añadiendo mejoras al *software*. Así, el ritmo de innovación en productos de *software* libre puede ser mayor que en productos de *software* propietario.

Uno de los problemas que enfrentan muchos proyectos de *software* libre es la llamada **tragedia de los comunes**. Aunque muchas personas se beneficien de un proyecto de *software* libre, los desarrolladores podrían no tener un incentivo para contribuir a él, al no beneficiarse directamente de su esfuerzo contribuyendo al proyecto. Muchos proyectos de *software* libre se enfrentan a dificultades para obtener financiación o conseguir que los desarrolladores le dediquen el tiempo adecuado. Existen algunos indicios de que Bitcoin podría estar enfrentándose a este problema ([2]).

Una exposición de los méritos de *software* libre pueden encontrarse en [10].

3. Base de datos pública

En el corazón de Bitcoin se encuentra una base de datos distribuida que contiene la posición de todas las direcciones de Bitcoin. Al tratarse de una base de datos distribuida, cada participante en la red (nodo) mantiene una copia de ella. Todas las copias de esta base de datos mantenidas por los nodos son consistentes entre sí por diseño.

[3] La mayoría de los proyectos son realmente bifurcadas muchas veces por usuarios que desean jugar con ellos o probar nuevas características. Sin embargo, bifurcaciones de grandes proyectos de software libre que dividen la base de desarrolladores, como la bifurcación de LibreOffice a partir de OpenOffice ([8]), son más bien raras.

Por otro lado, cada usuario tiene el control de sus propios fondos, a través de una clave privada criptográfica. Cuando un usuario desea enviar fondos a otro usuario, utiliza esta clave privada para firmar un mensaje indicando a quién desea enviar los fondos, así como la cantidad a enviar. El usuario emite una copia de este mensaje firmado a la red, y todos los participantes en la red reciben una copia del mismo. De este modo, cada nodo puede verificar de forma independiente la validez del mensaje y actualizar su base de datos interna en consecuencia[4].

En los sistemas financieros tradicionales, el valor está representado en bases de datos gestionadas por las instituciones financieras. Los usuarios deben confiar en que estas instituciones gestionen de manera adecuada estas bases de datos, y que no sean dañadas por atacantes ni internos ni externos. Los protocolos y procedimientos que guardan estas bases de datos financieras tradicionales no suelen ser revelados al público. En contraste, en Bitcoin la base de datos es pública y se crea un protocolo de *software* libre para mantener su seguridad. Este protocolo está diseñado para ser resistente contra atacantes que puedan formar parte de la red. Los usuarios de Bitcoin no tienen porque poner la confianza en terceras entidades: se dice que el sistema no requiere confianza *(trust-less)*.

Toda la información financiera que fluye a través de la red Bitcoin es pública, salvo las identidades detrás de las transacciones. Bitcoin no usa información personal para identificar a los titulares de los fondos, sino direcciones de Bitcoin. Las direcciones son cadenas de letras y números aparentemente aleatorios, tales como "13mckXcnnEd4SEkC27PnFH8dsY2gdGhRvM". En este sentido, Bitcoin es cómo hacer pública la información bancaria de todos los usuarios, pero manteniendo la identidad detrás de cada cuenta privada ([1]).

Aunque, en principio, las direcciones de Bitcoin no están asociadas a ninguna identidad, hay muchas técnicas para analizar la información pública de la red de Bitcoin y adquirir diferentes grados de conocimiento acerca de las direcciones Bitcoin y los usuarios detrás de estas (capítulo 13).

Bitcoin no es anónimo, e incluso podría decirse que es menos anónimo que los sistemas de pago tradicionales. En estos sistemas de pago tradicionales, por ejemplo, una empresa no puede conocer en qué gasta su salario un empleado, sólo el banco del empleado tiene esa información. Sin embargo, si un empleado recibiese su paga en bitcoins, su empleador podría ver dónde gasta esta paga simplemente siguiendo el rastro de las transacciones que surgen de la dirección donde la paga fue enviada. En este caso, el empleado podría seguir algunas prácticas para ocultar esta ruta de transacciones (capítulo 13).

En otros casos, la transparencia ofrecida por Bitcoin puede ser una ventaja. Un ejemplo es el caso de las entidades públicas donde la transparencia en el destino de los fondos podría ayudar a aumentar la calidad de la administración y evitar la corrupción. En el caso de las empresas privadas, un cierto nivel de transparencia puede ser beneficioso, por ejemplo para que los estados financieros pudieran ser verificados directamente en la base de datos distribuida. Los desarrolladores de criptomonedas están trabajando en progresos tecnológicos que pueden ayudar a resolver estos problemas (sección 8.5).

4. No es sólo la moneda, es la tecnología

La transferencia de valor ha sido tradicionalmente un proceso lento y muy manual. En esencia, Bitcoin es un protocolo para crear consenso distribuido. Este protocolo permite la transferencia de valor de forma segura en una forma que no requiere confianza en terceras partes: es una plataforma abierta para la transferencia de dinero. Pero la plataforma no

[4] El proceso es realmente más complicado para prevenir los ataques de doble gasto *(double spending)*, en los que un usuario envía diferentes mensajes a diferentes partes de la red. El mecanismo por el que Bitcoin previene los ataques de doble gasto es el tema del capítulo 7.

está limitada sólo al dinero: Bitcoin y protocolos similares pueden transferir cualquier activo digital (capítulo 12). Además esta tecnología es más barata y más rápida que la mayoría de las alternativas, lo que puede crear oportunidades para que se desarrollen nuevas aplicaciones.

La transferencia digital de valor permite la creación de contratos inteligentes *(smart contracts)*. Los **contratos inteligentes** son contratos que no requieren la interpretación o la intervención humana para llevarse a cabo. La ejecución de estos contratos se realiza de forma automática al ejecutar un programa de ordenador. Los contratos inteligentes son contratos cuyo cumplimiento está basado en propiedades matemáticas (criptografía), a diferencia de los contratos legales. La transferencia de valor digital mediante un sistema que no requiere confianza abre la puerta a nuevas aplicaciones que pueden hacer uso de los contratos inteligentes.

Una de estas aplicaciones son los agentes autónomos. Los agentes autónomos no deben confundirse con la inteligencia artificial. Los agentes autónomos son simplemente programas de ordenador sencillos, creados para una tarea específica. Un ejemplo es un programa que se ejecuta en la nube y que alquila espacio de almacenamiento y ofrece a sus clientes finales un servicio de almacenamiento de archivos. Hasta ahora los programas de ordenador no podían contener el valor: un programa informático no podía abrir una cuenta bancaria a su nombre. Con la introducción de Bitcoin, los programas de ordenador pueden controlar sus propios fondos y firmar contratos con proveedores de servicios en la nube, por ejemplo para alquilar almacenamiento y potencia de cálculo. Del mismo modo, este agente autónomo podría firmar contratos inteligentes con sus usuarios finales. El agente autónomo puede liquidar estos contratos inteligentes realizando los pagos al proveedor de la nube y recibiendo los pagos de sus usuarios finales en bitcoins ([5]). La sección 12.4 contiene una discusión más extensa de agentes autónomos.

Los agentes autónomos son sólo un ejemplo, y muchas más ideas innovadoras están siendo diseñandas (capítulo 12). Algunas de estas ideas pueden resultar no ser prácticas, pero tal vez algunas pueden llegar a convertirse en tecnologías establecidas. Un sistema descentralizado es un campo de pruebas ideal para estas tecnologías, ya que los innovadores no necesitan la aprobación de nadie para probar sus ideas: un sistema descentralizado permite la innovación-sin-permiso.

Bitcoin es un API *(Application Programming Interface)* para el dinero y la moneda bitcoin es sólo la primera aplicación. Bitcoin podría ser utilizado como una plataforma abierta para el intercambio de valor de la misma manera que Internet es una plataforma abierta para el intercambio de información. Puede ser utilizado como un protocolo sobre el cual otras aplicaciones pueden ser construidas, al igual que el correo electrónico, las páginas web o la voz sobre IP han sido diseñadas sobre el protocolo TCP/IP. De aquí viene la mayor parte del entusiasmo en torno a Bitcoin y tecnologías relacionadas. Independientemente de si Bitcoin tiene futuro como moneda, la tecnología ha demostrado que muchas aplicaciones son ahora posibles y los innovadores seguirán impulsando nuevas ideas. Bitcoin podría convertirse en una plataforma para la innovación financiera.

Una de las enseñanzas más importantes del economista Ronald Coase en "La naturaleza de la empresa" ([3]) ha sido la idea de que uno de los factores que contribuyó a la creación de empresas es los altos costes de transacción. Si no existiesen los costes de transacción, un empresario podría contratar cualquier bien o servicio que se necesite en el mercado, y esto sería eficiente, ya que un mercado eficiente conduciría al mejor precio para cualquier bien o servicio. Sin embargo, los costes de transacción, tales como la recopilación de información, costes de negociación, la vigilancia del contrato, los costes de mantener secretos comerciales, y así sucesivamente, pueden ser una parte importante del coste total de la contratación externa. Por esta razón, muchas veces es más barato para un empresario contratar empleados para producir los bienes intermedios necesarios para la consecución del producto final. Es por esta razón, argumenta Coase, que se crearon las grandes corporaciones. Los costes de transacción están también en el origen de los bienes públicos y la acción del gobierno.

El avance tecnológico introducido por Bitcoin puede abrir la puerta a unos menores costes de entrada y ejecución en los contratos digitales, por ejemplo a través de contratos inteligentes. La disponibilidad de contratos más eficientes puede hacer cambiar la razón de ser de las corporaciones y la acción del gobierno en algunos sectores económicos y algunos aspectos de la sociedad. ▮

Bibliografía

[1] Adam Back, 2014, Fungibility, Privacy & Identity. https://www.youtube.com/watch?v=3dAdI3Gzodo

[2] Danny Bradbury, 2014, Bitcoin Core Development Falling Behind, Warns BitcoinJ's Mike Hearn. CoinDesk. www.coindesk.com/ bitcoin-core-development-falling-behind-warns-mike-hearn/

[3] Ronald Coase, 1937, The Nature of the Firm. In Economica 4 (16): 386-405.

[4] Eldad Eilam, 2005, Reversing: Secrets of Reverse Engineering. John Wiley & Sons.

[5] Jeff Garzik, 2013, StorJ, and Bitcoin autonomous agents. http://garzikrants.blogspot.com/2013/01/storj-and-bitcoin-autonomous-agents.html

[6] Matthew Green, 2014, Attack of the week: OpenSSL Heartbleed. blog.cryptographyengineering.com/2014/04/attack-of-week-openssl-heartbleed.html

[7] Leslie Lamport, Robert Shostak, Marshall Pease, 1982, The Byzantine Generals Problem. In ACM Transactions on Programming Languages and Systems 4 (3): 382-401. http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

[8] Ryan Paul, 2011, Oracle gives up on OpenOffice after community forks the project. Arstechnica. http://arstechnica.com/information-technology/2011/04/oracle-gives-up-on-ooo-after-community-forks-the-project/

[9] Kevin Poulsen, 2014, Behind iPhone's Critical Security Bug, a Single Bad 'Goto'. Wired. www.wired.com/2014/02/gotofail/

[10] Eric Raymond, 2001, The Cathedral & the Bazaar. O'Reilly Media.