BITCÓIN: ¿UNA REVOLUCIÓN? (*)

Guillaume HAERINGER
Baruch College

Hanna HALABURDA (**)
Bank of Canada

Resumen

Los términos bitcóin, criptomoneda, *blockchain* o «contrato inteligente» están en boca de todos, y muchos predicen que estas tecnologías van a suponer una revolución en nuestras vidas. Pero la aparente complejidad del bitcóin y de la tecnología asociada a él hace que resulte difícil participar en el debate. El objetivo de este artículo es ofrecer una descripción no técnica de este nuevo fenómeno, esbozando respuestas a muchas preguntas frecuentes (como el consumo de electricidad del bitcóin, o la necesidad de invertir una cantidad de recursos ineficiente en minar), y derribar algunos de los mitos que rodean al bitcóin y a la tecnología de cadena de bloques (por ejemplo, que es 100 por 100 segura).

Palabras clave: bitcóin, tecnología de cadena de bloques, minería ineficiente, consumo de electricidad.

Abstract

Today more and more people talk about Bitcoin, cryptocurrencies, blockchain, or smart contracts, and many predict that these technologies will revolutionize our lives. But the apparent complexity of Bitcoin and its related technology makes it hard to participate to the debate. The purpose of this chapter is to offer a non-technical description of this new phenomenon, giving answers to many common questions (e.g., the electricity consumption of Bitcoin, or the necessity of "wasteful" mining) and debunking some of the myths surrounding Bitcoin and the blockchain technology (e.g., that it is 100 por 100 tamper proof).

Key words: bitcoin, blockchain technology, wasteful mining, electricity consumption.

JEL classification: D80, G20, O30, 033.

I. INTRODUCCIÓN

En 2008 apareció en Internet un artículo en el que se describía un sistema monetario (es decir, una «moneda») totalmente descentralizado. El artículo estaba firmado por Satoshi Nakamoto, un seudónimo. El/la/los inventor/a/es del sistema y redactor/a/es de la propuesta bautizaron la moneda con el nombre de Bitcóin (1). Diez años más tarde el Bitcóin se ha convertido en una cuestión familiar, tratada periódicamente en la prensa, blogs y otros medios de comunicación. Para muchos, el Bitcóin es una revolución. Cuando menos esta nueva «moneda» presenta rasgos llamativos. La volatilidad de su cotización no responde a ningún patrón conocido, desafiando tanto a analistas financieros como a eruditos en la materia. Existe la preocupación de que las herramientas de análisis de activos tradicionales no sean adecuadas en este caso (véase, por ejemplo, Urquart, 2016). Muchos responsables de bancos centrales y reguladores, recelando de las consecuencias de tal volatilidad y falta de control, están interesándose activamente en todo lo que rodea a esta moneda. ¿Qué es lo que hace del Bitcóin una «revolución»?

A primera vista, el Bitcóin parece revolucionario porque ofrece un sistema dinerario sin la intervención de un «tercero de confianza». Pero, en cierto modo, constituye una vuelta a lo básico. Todos los sistemas de dinero primigenios funcionaban sin un tercero de confianza. Entonces, ¿qué diferencia al Bitcóin?

Solemos pensar en el dinero como un medio de pago bajo el control de autoridades y terceros de confianza, tales como gobiernos, bancos, bancos centrales, cooperativas de crédito, etcétera. Pero éstos son fenómenos bastante recientes en la historia del dinero (véase, por ejemplo, Ferguson, 2009 o Halaburda y Sarvary, 2016). En esencia, el dinero (o un sistema monetario) no es más que algo que utiliza un grupo de personas para facilitar el intercambio de productos y servicios. Si nos remontamos a los primeros tiempos, el dinero estaba representado por conchas marinas, dientes de animales y, más tarde, piezas de metales preciosos. Dichas formas de dinero no precisaban de ninguna autoridad ni de ningún tercero de confianza (2).

Con el tiempo, las monedas emitidas por reyes y emperadores incorporaron un sello para certificar la cantidad de metal acuñado en la moneda. Tal certificación facilitaba las transacciones, pues ahorraba tiempo y tener que pesar el metal cada vez que se realizaba una transacción. Ahora bien, solo funcionaba si la certificación era digna de confianza.

Pero el metal pesa, especialmente si no nos limitamos al oro y la plata. En la Suecia del siglo XVII, el cobre era el metal

empleado para acuñar monedas. Intercambiar valor de cierta entidad implicaba portar consigo chapas de cobre de varios kilos de peso. Los terceros de confianza, como los bancos, y más tarde los bancos centrales, hicieron más sencillo el comercio con la introducción del papel moneda, más fácil de transportar y usar. El valor asignado al papel moneda estuvo en un principio relacionado con la promesa de los bancos de canjear los billetes por una cantidad especificada de metal. Pero finalmente, todo se reducía a saber si una unidad de valor dada sería reconocida como pago en la siguiente transacción. Fue esto lo que hizo que el papel moneda también triunfase como medio de pago una vez que los bancos abandonaron el patrón oro y dejaron de referenciar el valor de los billetes a una cierta cantidad de metal.

El papel moneda resulta un medio de pago más cómodo que las conchas marinas o las piezas de oro. Pero mientras que las conchas o el oro son, por naturaleza, difíciles de obtener (y, en el caso del segundo, imposibles de crear, pese a los denodados esfuerzos de generaciones de alquimistas), en el caso del papel moneda se hace necesaria una autoridad responsable de emitir la cantidad justa de él para garantizar un nivel de escasez adecuado, y de perseguir su falsificación.

Con la llegada de la era tecnológica, el dinero digital adopta la forma de ceros y unos, incorporándose físicamente a tarjetas y chips. Su mayor facilidad de uso está desplazando incluso al papel moneda. Su comodidad se refleja en la disminución del efectivo utilizado para pagar por las compras, al tiempo que se generaliza el uso de tarjetas de crédito y débito. Paralelamente, el servicio de garantizar la escasez, prestado por un tercero de confianza, cobra aún más importancia en el caso de las formas digitales de dinero. Esto se debe a que realizar copias perfectas (es decir, falsificaciones) de dinero digital es muy barato. Dicha reproducción permitiría utilizar más de una vez la misma moneda digital para pagar. A fin de impedir este *doble gasto*, todos los sistemas de pago digitales anteriores al Bitcóin dependían de un tercero de confianza (es decir, un banco) que controlase todo el dinero gastado y garantizase que nadie pudiese utilizar el mismo dinero varias veces.

La innovación aportada por el sistema del Bitcóin estribó en que, por primera vez, ofrecía un *dinero digital* sin un tercero de confianza. En las siguientes secciones describimos cómo es capaz de lograrlo. Pero antes de entrar en materia, conviene mencionar que construir un sistema totalmente descentralizado (es decir, que no precise de un tercero de confianza) de dinero digital ha sido un reto largamente acariciado por la comunidad criptográfica, remontándose los primeros intentos hasta, al menos, los años 1980. Aquellos intentos lo abordaron como una cuestión puramente criptográfica y se centraron en soluciones de criptografía. Pero el Bitcóin fue el primero en tener éxito, y ello se debió a que combinó herramientas de criptografía y sistemas de incentivos para impedir el «doble gasto».

En las secciones segunda y tercera se explica más detalladamente el funcionamiento del Bitcóin, sin adentrarnos en complejidades técnicas, mientras que las secciones cuarta y quinta abordan los usos actuales y potenciales del Bitcóin y las tecnologías que han surgido inspiradas por él.

II. EL PROTOCOLO BITCÓIN

El Bitcóin es un sistema digital de dinero formado por una moneda a la que se denomina *Bitcóin* (representada en notación escrita con una *b* minúscula y con el símbolo ฿) y dos tipos de actores: los usuarios y los *mineros* (3). El Bitcóin es un sistema de dinero puramente *digital*, lo que significa que carece de una versión numismática en forma de monedas o billetes (4).

Por usuario del Bitcóin se entiende cualquier persona o entidad que posea o reciba bitcoines, y *minero* es cualquier persona o entidad que registre y valide transacciones. Desde la perspectiva de un usuario, podría parecer que el sistema del Bitcóin no se diferencia demasiado del método de anotación en cuenta de los bancos (si bien con servicios muy limitados: solo admite depósitos y transferencias). No obstante, la mecánica de validación y liquidación de las transferencias es diferente.

1. Monederos y el *blockchain*

Para convertirse en usuario del sistema del Bitcóin, es necesario abrir una cuenta, algo parecido a tener una tarjeta de débito con un PIN. Cualquiera puede generar fácilmente una cuenta (o más de una) de bitcóins en webs específicas como bitaddress.org o blockchain.info. Cuando un usuario genera una cuenta de Bitcóin, obtiene una cadena de caracteres y un número. Esta cadena es la *dirección de Bitcóin*, el equivalente a

un número de tarjeta de débito o al número de cuenta bancaria, y tiene la siguiente apariencia (5):

12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX.

Para enviar bitcoines a alguien necesitamos conocer la dirección de esa persona, nuestra dirección y nuestra *clave privada de Bitcóin*. Esta última se asemeja un poco al PIN de nuestra tarjeta de débito. Pero en el Bitcóin, ese PIN no se compone de 4 dígitos, sino que es mucho más largo. Tiene ¡77 dígitos! Para hacerlo más «fácil», este número suele representarse con una cadena de caracteres, similar a una dirección de Bitcóin. He aquí un ejemplo de una clave privada de Bitcóin (6):

873D79C6D87DC0FB6A5778633389.

Conjuntamente, la dirección y la clave privada forman el *monedero de Bitcóin*. Obsérvese que en la terminología del Bitcóin no se emplea el término «cuenta», sino «dirección» (o «monedero»). Ya estamos listos para empezar: los usuarios tienen números de cuenta (la dirección de Bitcóin) y un PIN (la clave privada de Bitcóin) que les permiten gastar o recibir bitcoines. A diferencia de las tarjetas de débito, es posible tener un número prácticamente *ilimitado* de monederos de Bitcóin. Se puede crear un nuevo monedero Bitcóin para cada transacción. Pero, si no hay bancos, ¿cómo se almacenan los bitcoines? La respuesta está en una de las palabras que últimamente circula de boca en boca: el *blockchain*, o cadena de bloques.

Para empezar, el *blockchain* del Bitcóin es un fichero informático (7). Más exactamente, es un libro-registro que contiene la historia completa de todas las transacciones ejecutadas con el Bitcóin desde su creación. Las transacciones en la cadena se agrupan en bloques (series), y la secuencia de bloques constituye la cadena de bloques. De ahí el nombre *blockchain*. Cada vez que un usuario envía bitcoines a otra dirección, esa transferencia se almacena en la cadena.

A diferencia de los números de cuenta en un banco, la cadena de bloques es *pública*: cualquiera puede acceder a ella. Lo que no contiene la cadena, sin embargo, son los nombres de los propietarios de las direcciones de Bitcóin almacenadas en ella (8).

Observación 1. Mucha gente cree que, puesto que la cadena de bloques solo contiene direcciones de Bitcóin, es una forma de pago anónima. No es exacto. Los informáticos han demostrado que, a través de un análisis minucioso de la cadena y triangulando su información con otras fuentes, es posible identificar algunos usuarios (véase Androulaki et al., 2013).

Para conocer el saldo de una dirección tenemos que analizar la totalidad de la cadena en busca de dicha dirección, y el saldo es simplemente el resultado de la suma de todas las transacciones de entrada menos la suma de todas las transacciones de salida (no necesitamos conocer la clave privada asociada a dicha dirección). Existen una serie de webs que lo hacen por lo que no es necesario descargar la cadena entera y hacer una búsqueda. Las mismas webs también ofrecen herramientas para enviar fácilmente bitcoines de una dirección a otra.

Hay decenas de miles de ordenadores en el mundo con una copia de la cadena mantenidos por personas denominadas *mineros* (su actividad se describe en la siguiente sección) (9). La existencia de múltiples copias de la cadena aporta cierta confianza al sistema. Dado que cada copia de la cadena contiene los bitcoines asociados a cualquier monedero, no hay riesgo de pérdida debido a un fallo informático. No obstante, la existencia de múltiples copias no la protege frente a manipulaciones y fraudes. En la tercera sección veremos que hay otras propiedades del Bitcóin que contribuyen a evitarlos.

Observación 2. Dado que el Bitcóin es un sistema que funciona sin terceros, las tenencias de bitcoines no están garantizadas. Todo lo que necesita un ladrón para robar es acceder a tu monedero (la dirección de Bitcóin y la clave privada). En esto se diferencia de las tarjetas de crédito o las cuentas bancarias, que suelen incluir cierta garantía frente a robos.

Aún más importante, si un usuario pierde su clave privada de Bitcóin, no existe forma alguna de recuperarla. Los bitcoines guardados en el monedero asociado se perderían para siempre. Se cree que unos cuatro millones de bitcoines se han perdido así desde 2008 (10). *Eso no ocurre con las cuentas bancarias. Una persona que pierde el PIN de su tarjeta de crédito (o su número de cuenta) puede pedir al banco que emita un nuevo PIN una vez que acredite su identidad (p. ej., mostrando su pasaporte).*

Así es como se almacenan los bitcoines. ¿Pero cómo se consiguen? La manera más frecuente de conseguir bitcoines es comprarlos pagando con alguna moneda de curso legal, como euros o dólares. Existen webs —llamadas mercados o *exchan-*

ges— creadas con ese fin (11). Una vez que has comprado bitcoines, le ordenas al mercado que los envíe a tu cuenta de Bitcóin… y ¡ya está! Otra manera de conseguir bitcoines es realizar una venta y cobrar el precio en bitcoines. Existe una tercera vía de adquirir bitcoines: *minarlos*.

2. Minería

En el sistema Bitcóin, la minería es una actividad que entraña dos vertientes: procesar transacciones y generar nuevos bitcoines. Por cada bloque añadido a la cadena, hay un minero que fue el primero en construir ese bloque y enviárselo a todos los demás mineros con el mensaje: «por favor, añade este nuevo bloque a la cadena». Uno de los aspectos clave del Bitcóin es que existe competencia entre los mineros para ser quien construya el siguiente bloque. Cada vez que un bloque es añadido a la cadena, se crean nuevos bitcoines, que constituyen lo que se denomina la *recompensa* otorgada al minero por crear el bloque. Dicho minero también cobra todas las comisiones de transacción asociadas a las transacciones integrantes del bloque.

Debido a que existe competencia, crear un bloque de transacciones no es una tarea sencilla: no basta simplemente con crear una lista de transacciones y enviársela a los demás mineros. En esta sección explicamos qué deben hacer los mineros para construir un bloque. La sección tercera se centra en la competencia: cómo funciona y por qué constituye un elemento *necesario* del sistema Bitcóin.

Enviar bitcoines a una dirección de Bitcóin consiste en enviar un mensaje a la red Bitcóin a través de Internet (12). Simplificando un poco, podemos decir que dicho mensaje contiene:

- La dirección del remitente.
- La dirección del destinatario.
- La cantidad de Bitcóins a transferir.
- Las comisiones que el remitente pagará al minero que procese la transacción. La cantidad de la comisión la decide el remitente (puede ser cero).
- Una «firma» del remitente.

Los mineros observan las transacciones que aún no han sido procesadas (es decir, que no están en la cadena) y pueden elegir qué transacciones incluir en el bloque que propondrán. Aquí es donde entran en juego las comisiones: un minero estará más interesado en procesar transacciones que conlleven comisiones más elevadas.

Por cada transacción seleccionada, el minero, que posee una copia de la cadena, comprueba primero si la transacción es válida. Para ello, el minero verifica si la dirección del remitente tiene el saldo de bitcoines que pretende enviar mediante el análisis de la cadena y la comprobación de que esa dirección ha recibido los bitcoines en el pasado y no los ha gastado aún. El minero también se asegura de que el remitente sea el propietario de la dirección desde la que se transferirán los bitcoines. Aquí es donde la «firma» tiene relevancia. La firma se genera utilizando la clave privada y el mensaje. Las herramientas criptográficas son brillantes: permiten verificar que la firma se ha generado mediante la clave privada asociada a la dirección: ¡sin necesidad de conocer dicha clave privada! En otras palabras, la firma permite al minero autenticar al remitente, es decir, cerciorarse de que el remitente está en posesión de la clave privada asociada a la dirección del remitente (y, por tanto, probablemente es el propietario de esa dirección) (13). El hecho de que la firma se genere utilizando no solo la clave privada sino también el mensaje implica que la firma cambia con cada transacción. Por tanto, cualquier transacción que reutilice una firma de una transacción anterior será inmediatamente rechazada por los mineros como fraudulenta.

Una vez que el minero haya verificado las transacciones y las haya incluido en su bloque, añadirá una nueva transacción especial que consiste en asignarse a sí mismo la recompensa del bloque: bitcoines de nueva creación (en una cantidad que se especifica en el protocolo Bitcóin). Casi tenemos un bloque listo para ser agregado a la cadena. Lo que falta es un número, necesario para «emparejar» el nuevo bloque con la cadena, una operación semejante a hacer coincidir dos piezas en un rompecabezas: el nuevo bloque debe ser «compatible» con la cadena, pues de otro modo los demás mineros rehusarán añadir el bloque a sus copias de la cadena.

Dicho número es una solución a un difícil problema numérico que no puede resolverse por habilidad (14). La única manera de resolverlo es por prueba y error: intentar todos los números posibles, uno tras otro, hasta que se da con el correcto (veremos en la siguiente sección por qué es difícil). Ese problema depende de

la información contenida en la actual cadena y en el (potencial) nuevo bloque. Conocer la solución correspondiente al bloque anterior no ayuda a encontrar la solución del siguiente bloque. El problema es difícil, pero una vez que se encuentra la solución, es muy fácil comprobar que efectivamente es el número correcto. En términos muy sencillos, es como dar con la raíz cuadrada de una cifra de muchos dígitos utilizando una calculadora que solo realiza multiplicaciones. Lleva tiempo encontrar manualmente la raíz cuadrada de, digamos, 1.619.220.498.932.521, pero es muy fácil comprobar que 40.239.539 es la solución. De forma análoga, aunque resolver el cubo de Rubik es difícil, comprobar que ha sido resuelto es muy fácil. La idea de que un bloque de transacciones solo pueda añadirse a la cadena después de que un minero haya encontrado una solución a un difícil problema se denomina *proof-of-work* (prueba de trabajo).

Dado que un minero no tiene más opción que probar la mayor cantidad de números hasta dar con el correcto, encontrar la solución lleva tiempo. El Bitcóin está diseñado de modo que, de media, encontrar la solución lleva a uno de los mineros de la red unos diez minutos. Algunas veces tardará solo unos segundos (si el minero tuvo suerte), y en otras llevará veinte o treinta minutos. Pero la media es de diez minutos.

Una vez que un minero ha encontrado la solución al problema numérico, el bloque está listo para enviarse a los demás mineros. Si el minero es el primero en anunciar la creación de un nuevo bloque, los demás mineros añadirán el bloque a su copia de la cadena (una vez comprobado que contiene transacciones autorizadas y que la solución es correcta). Si al comienzo todos los mineros tenían la misma copia de la cadena y todos añaden el mismo bloque, todos terminarán teniendo la misma nueva versión de la cadena.

Un aspecto importante de la minería de bloques es el siguiente. Supongamos que una minera, llamémosla Alicia, estaba trabajando en un bloque (es decir, buscando la solución del problema) cuando un nuevo bloque es anunciado y añadido a la cadena. Esto significa que Alicia ha perdido la pugna, y debe comenzar nuevamente de cero —buscando una solución al siguiente nuevo bloque—. Esto es así por dos motivos. Primero, el bloque recién añadido puede contener algunas transacciones que Alicia estaba tratando de procesar. De modo que Alicia tendría que actualizar la lista de transacciones que desea procesar. Segundo, y más importante, como hemos explicado más arriba, el problema que Alicia tiene que resolver depende de la cadena. Dado que la cadena ha cambiado (se ha añadido un bloque) el problema sobre el que Alicia estaba trabajando ya no es el correcto. Por tanto, los esfuerzos de Alicia por encontrar la solución a su antiguo problema ya no sirven de nada.

Cada vez que se añade un bloque a la cadena, el minero ganador obtiene una *recompensa* además de las comisiones asignadas a las transacciones procesadas. Esta recompensa se compone de nuevos bitcoines, creados *ex nihilo* (de la nada). Esta es la única fuente de nuevos bitcoines. En el momento de crearse el sistema, la recompensa era de 50 bitcoines. Por diseño, la recompensa se divide entre dos, aproximadamente cada cuatro años. En 2018, la recompensa es de 12,5 bitcoines y se espera que disminuya hasta 6,25 bitcoines en torno a mayo de 2020. Alrededor de mayo de 2140, la recompensa caerá a 0. Después de esa fecha, no se podrán crear más bitcoines y la única fuente de ingresos para los mineros serán las comisiones por transacción, es decir, la cantidad que los usuarios paguen a los mineros por procesar sus transacciones.

III. EL JUEGO DEL BITCÓIN

La minería consume electricidad y requiere invertir en potencia de computación. Recientemente, tanto el consumo de electricidad como la inversión requerida han registrado un aumento significativo. Los ordenadores especializados para minería cuestan varios miles de dólares. Y a finales de 2017, se estimaba que la minería de Bitcóin consumía tanta energía como Dinamarca (15). ¿Por qué sucede esto?

La explicación es que a los mineros les compensa. Sus incentivos reflejan la naturaleza competitiva de la minería. Puesto que solo el primer minero en encontrar la solución consigue la recompensa de nuevos bitcoines y las comisiones, le interesa invertir en más potencia computacional para ser más rápido que los demás. Esto empuja a su vez a los otros mineros a invertir para ser aún más rápidos. El propio diseño del «juego» (es decir, el ganador se lleva todo el premio) conduce a una *escalada armamentista* entre los mineros, exacerbada cada vez que el precio del Bitcóin aumenta. A finales de 2017 el valor de un bitcoin ascendía aproximadamente a 16.000 dólares, y la recompensa por minar era de unos 200.000

dólares. Con cifras tan elevadas, la recompensa potencial hace que merezca la pena invertir en un ordenador potente.

El resultado es que hay cada vez más mineros, con equipos más potentes, que consumen cada vez más energía. De forma interesante, la mayor parte de este esfuerzo, esta inversión y este consumo energético se desperdicia. Varios miles de mineros consumen energía en busca de una solución al problema numérico, pero solo uno logrará ser quien inicie el próximo bloque. Ninguno de los cálculos realizados por los demás mineros entrará en la cadena. Si la cuestión se redujese a registrar transacciones en la cadena, podría conseguirse con un uso de recursos mucho menor. ¿Tiene sentido, o se trata de un fallo en el sistema que debe ser arreglado?

Lo cierto es que, dentro del sistema Bitcóin, este esfuerzo «baldío» en computación desempeña un papel importante en la seguridad del sistema. Todos los cálculos realizados por los mineros «perdedores» hacen que aumente el coste de ganarse el derecho a añadir un nuevo bloque a la cadena, lo que evita el doble gasto. Para demostrarlo, imaginemos la siguiente situación. Zoe compra una bicicleta con sus bitcoines. Para ello, envía bitcoines al vendedor y a cambio este le entrega la bicicleta. Por tanto, la transferencia de bitcoines desde la dirección de Zoe a la del vendedor aparecerá en la cadena. Supongamos ahora que Zoe no es honrada y pretende recuperar sus bitcoines sin devolver la bicicleta al vendedor. Para hacerlo, necesitaría *borrar* la transacción de la cadena (16). Modificar esto en su cadena no será suficiente, habida cuenta del diseño del Bitcóin: los otros mineros solo *añaden* bloques a sus copias de la cadena, pero no pueden *borrar* o *reescribir* bloques. Lo que Zoe necesitaría hacer es convencer a los demás mineros de que tienen una copia inexacta de la cadena y que la copia exacta es la que ella construyó (que coincide perfectamente con la verdadera salvo por el hecho de que no contiene su transacción).

1. Bifurcaciones

Pero, un momento: ¿por qué iban a aceptar los otros mineros sustituir una cadena por otra? Por puro diseño, el Bitcóin no funcionaría si ello no fuera posible. La razón es que, a veces, tener dos (o más) versiones diferentes de la cadena es inevitable. He aquí el porqué.

Puede suceder que dos mineros, digamos, Alicia y Bob, encuentren la solución para el bloque que están procesando casi al mismo tiempo. También, dado que depende de cada minero seleccionar las transacciones que procesa, es muy probable que el bloque de Alicia y el de Bob no sean idénticos; esto es, que no contengan las mismas transacciones.

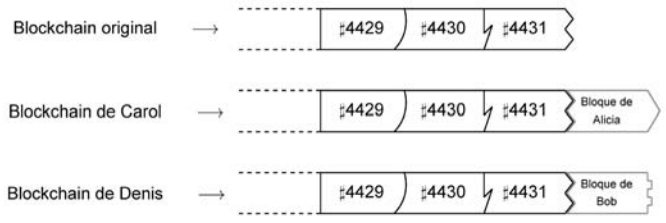
Puesto que las comunicaciones en Internet no son instantáneas, algunos mineros recibirán el bloque de Alicia antes que el de Bob, mientras que otros mineros recibirán antes el de Bob que el de Alicia (17). ¿Qué ocurriría en este caso? Consideremos el caso de una minera, Carol, que recibe antes el bloque de Alicia. Después de comprobar la validez del bloque, lo añadirá a su copia de la cadena. Unos pocos segundos después, recibe el bloque de Bob. La solución de Bob se obtuvo para la cadena previa a añadirle el bloque de Alicia; una vez añadido éste, el bloque de Bob (con su solución al problema numérico) deja de ser compatible, como sucede cuando dos piezas de un rompecabezas no encajan. Así pues, Carol rehúsa añadir el bloque de Bob a la cadena.

Al mismo tiempo hay otro minero, Denis, que se encuentra con una situación simétrica. Recibió primero el bloque de Bob y lo añadió a su copia de la cadena. Cuando llega el bloque de Alicia unos segundos después, Denis lo encontrará inválido y lo rechazará. Así, ahora tenemos dos copias competidoras de la cadena: una con el bloque de Alicia y otra con el bloque de Bob. El gráfico 1 ilustra esta situación.

En el ejemplo que se muestra en el gráfico 1, la cadena original acaba con los bloques 4429, 4430 y 4431, siendo el bloque 4431 el último bloque añadido a la cadena. Podemos ver que los bloques encajan unos con otros como en un rompecabezas. Las formas de los bloques en el gráfico reflejan el hecho de que la so-

GRÁFICO 1

DOS CADENAS COMPETIDORAS



lución del problema numérico es lo que hace compatible al bloque con la cadena (recuérdese que el problema depende tanto de la cadena como del bloque que se está procesando).

Ambos bloques, el de Alicia y el de Bob, pueden ser añadidos a la cadena, ya que la solución que encontraron hace a su bloque compatible con la cadena original. Pero una vez que se ha añadido el bloque de Alicia, no podemos añadir el bloque propuesto por Bob: ya no encaja con la nueva cadena (la de Carol). Algo similar sucede si en lugar de añadir el bloque de Alicia añadimos el de Bob. Si queremos añadir el bloque de Alicia al final de la cadena de Denis, necesitamos encontrar una nueva solución de modo que la parte izquierda del bloque de Alicia encaje con la parte derecha del bloque de Bob (18).

En la jerga de Bitcóin, cuando hay dos o más cadenas competidoras, se dice que la cadena se ha bifurcado (*forked*). Sucede más o menos una vez a la semana. ¿Qué ocurre entonces? Obviamente, Alicia intentará añadir un bloque a la cadena de Carol. No tiene interés alguno en la cadena de Denis porque la recompensa de Alicia aparece en la cadena de Carol, pero no en la versión de la cadena que tiene Denis. Lo mismo le ocurre a Bob, quien trabajará sobre la cadena de Denis. A los demás mineros, les será indiferente. Algunos trabajarán sobre la cadena de Carol y otros sobre la de Denis. Dado que el tiempo necesario para encontrar la solución del siguiente bloque nunca es exactamente diez minutos, tarde o temprano una de las dos versiones de la cadena (la de Carol o la de Denis) será más larga, es decir, constará de más bloques. La convención en el sistema Bitcóin es que los mineros siempre se enfocan en la cadena más larga. Esto garantiza que a largo plazo exista consenso sobre cuál es la cadena «verdadera». Por tanto, la cadena más larga será la ganadora, y la otra versión de la cadena quedará *huérfana*.

Observación 3. Una transacción que aparece en una versión huérfana de la cadena pero no en la versión «ganadora» de la cadena no se pierde. Para los mineros que trabajan en esta última cadena, dicha transacción sigue estando en el pool *de transacciones aún no procesadas.*

Dado que la cadena en ocasiones puede bifurcarse, la mayoría de la gente esperará algunos bloques antes de considerar que una transacción ha quedado registrada en la cadena. Si yo recibiese bitcoines y esa transacción estuviera almacenada en el último bloque en ser añadido a la cadena, casi todas las contrapartidas rechazarían mis bitcoines si intentase gastarlos inmediatamente. Solo aceptarían mis bitcoines si apareciesen en el sexto, séptimo u octavo,… bloque anterior al último (lo habitual es esperar al menos seis bloques, es decir, en torno a una hora tras haberse procesado la transacción). Así pues, los pagos en bitcoines no son completamente instantáneos.

2. Reescribiendo la historia

Volvamos a nuestro caso inicial: Zoe se compró una bicicleta que pagó con bitcoines y desea «borrar» su pago. Para ello necesita dar los siguientes pasos:

1. (*Fácil*) Localizar el bloque en el que se encuentra la transacción.
2. (*Difícil*) Reconstruir el bloque sin su transacción (y, de esa forma, resolver el problema numérico de nuevo).
3. (*Extremadamente difícil*) Añadir los bloques que vinieron más tarde (resolviendo el problema numérico para cada uno de ellos) y ser *lo bastante rápida* para que la cadena que construya supere en longitud a la cadena original (y así los demás mineros opten por trabajar sobre su cadena).

El punto 3 es lo que hace del Bitcóin un sistema muy difícil y costoso de hackear. Durante el tiempo que Zoe construye bloques en su versión de la cadena, los demás mineros no permanecen de brazos cruzados. Siguen trabajando en la cadena principal. Lo que determina la probabilidad de que su ataque triunfe es su cuota de potencia de computación respecto a la potencia de computación total de todos los mineros de Bitcóin. Por ejemplo, si existen 10.000 mineros, todos con el mismo equipo de minería, cada minero tiene un 0,01 por 100 de potencia de computación.

Si Zoe posee una cuota pequeña de la potencia computacional total, es extremadamente improbable que sea capaz de resolver varios problemas a mayor velocidad que el resto de mineros. Una mayor cuota de potencia aumentará las probabilidades de éxito. Y llegar a reunir el 50 por 100 de la potencia de computación le garantiza que conseguirá construir una cadena competidora más larga (19). Pero semejante potencia computacional es muy cara de adquirir y de operar: ¡equivaldría a pagar la

factura de electricidad de media Dinamarca! Nótese que técnicamente no es imposible falsear o reescribir transacciones. Simplemente, es improbable y muy costoso. Así pues, a los atacantes potenciales no les sale rentable.

El mecanismo de seguridad de Bitcóin tiene dos propiedades interesantes que podrían parecer contraintuitivas. Primero, la existencia de un gran número de mineros «perdedores» que ven «desperdiciado» su esfuerzo de computación hace al Bitcóin más seguro frente a ataques. Segundo, cuando el precio del Bitcóin aumenta, también se refuerza la seguridad del sistema. Para comprender el primer punto, compararemos los siguientes dos escenarios en los que un atacante (a quien hemos denominado Zoe) está construyendo una versión diferente de la cadena:

– *Escenario A:* Además del atacante, hay 10 mineros honrados (es decir, mineros trabajando en la verdadera cadena). Es decir, solo existen 11 mineros en la red Bitcóin.

– *Escenario B*: Además del atacante, hay 1.000 mineros honrados (es decir, hay 1.001 mineros en total).

Por simplicidad, asumimos que cada minero en cada escenario está equipado con una computadora idéntica, esto es, todos tienen la misma potencia de computación nominal.

En cada escenario *A* y *B*, la versión honrada de la cadena crecerá aproximadamente a la misma velocidad, tanto si el atacante construye su propia versión de la cadena como si continúa trabajando en la cadena honrada —de media, un bloque cada diez minutos. Esta característica es subyacente al protocolo Bitcóin. La media de diez minutos se obtiene ajustando la dificultad del problema a resolver. Si no se ajustara la dificultad del problema, un mayor número de mineros con mayor potencia de computación encontrarían soluciones a los problemas, y minarían nuevos bitcoines más rápido. Es lo mismo que sucede cuando, por ejemplo, extravías las llaves de casa. Cuanta más gente haya buscándolas, antes las encontrarán. A fin de mantener el ritmo de producción de nuevos bitcoines estable (de media), el protocolo Bitcóin ajusta periódicamente la dificultad de minarlos. Como consecuencia, la dificultad del problema depende del número *total* de mineros (es decir, la potencia de computación total dedicada a la minería).

Entonces, ¿cuál es la diferencia entre el escenario *A* y el *B* para nuestro atacante? Como en el escenario *B* existe más potencia computacional destinada a la minería, el problema es mucho más difícil. Esto significa que para el atacante, que trabaja *aisladamente* en su versión de la cadena, encontrar soluciones a los problemas en el escenario *B* le llevará mucho más tiempo que en el escenario *A*. Y por consiguiente, bajo el escenario *B*, tiene *muchas menos probabilidades* de éxito en su intento de construir una cadena competidora más larga.

En ambos escenarios, por cada bloque solo hay un minero que gana la competición, más o menos cada diez minutos. Pero lo que importa es que en el escenario *A* hay solo nueve «perdedores» que desperdicien su esfuerzo de computación, mientras en el escenario *B* hay 999 perdedores, con lo que el esfuerzo de computación que se gasta en vano es mucho mayor. Pero cuantos más «perdedores» haya, más difícil es el problema a resolver, y por tanto más difícil es atacar el sistema, y más seguro es el Bitcóin. Esta es la razón de que la energía desperdiciada (por los mineros que pierden la competición) sea un elemento crucial del sistema Bitcóin.

Esto nos lleva a la segunda propiedad del mecanismo del Bitcóin: cuando el precio del Bitcóin aumenta, se hace incluso más improbable y más costoso reescribir la historia de la cadena. Un Bitcóin más caro significa una recompensa más valiosa por minar, y así más mineros verán rentable invertir en más potencia de computación para participar en la competención para encontrar los nuevos bitcoines. Esto incrementa la potencia computacional total destinada a minería (y también el consumo total de energía relacionado con la minería), y, por ende, la dificultad de los problemas a resolver. Ahora bien, esto significa que, o bien la proporción de la potencia de computación del atacante disminuye, lo que hace disminuir paralelamente su probabilidad de éxito, o bien se obliga al atacante a adquirir y operar más potencia de computación para mantener su cuota de potencia computacional, lo que es caro.

La posibilidad de obtener la recompensa del bloque implica que siempre habrá otros muchos mineros, y añadir un nuevo bloque solo podrá hacerse tras cálculos intensivos. Esto hace también que crear cadenas alternativas sea igual de caro, y, por tanto, que resulte virtualmente imposible que la reescritura de la historia triunfe y, al mismo tiempo, sea rentable. Por tanto, Zoe

se queda con la bicicleta y no intenta recuperar sus bitcoines…

3. Seguridad frente a energía desperdiciada

Como ya hemos visto, hay dos tipos de bifurcaciones: accidentales y deliberadas. Las bifurcaciones accidentales son una parte natural del sistema Bitcóin. Surgen como consecuencia del hecho de que Bitcóin es un sistema distribuido, y del mecanismo de consenso que Bitcóin usa —prueba de trabajo— para garantizar la consistencia de este libro-registro distribuido. Cuando por accidente aparecen múltiples cadenas, todos desean que la multiplicidad se resuelva lo antes posible. La regla de «seguir la cadena más larga» cumple esta finalidad, pues permite con fluidez que todos los mineros se coordinen en una de las ramas de la bifurcación.

Pero en el caso de las bifurcaciones deliberadas, tal regla de coordinación no es suficiente, pues el atacante podría tener la tentación de generar una cadena más larga a base de transacciones fraudulentas. El hecho de que las bifurcaciones puedan ser inocuas podría ayudar a un atacante a ofrecer una historia alternativa sin ser detectado como tal. La costosa minería, sin embargo, hace que los intentos de generar tales bifurcaciones deliberadas tengan escasas probabilidades de triunfar y salgan muy caros, por lo que no resultará rentable para el atacante.

Así, aunque la minería consume enormes cantidades de energía, y hay quien podría pensar que la mayoría de dicho gasto es un «desperdicio», debería verse como el precio a pagar por la seguridad del sistema sin un tercero de confianza. En el sistema Bitcóin, este consumo desperdiciado no es un fallo, sino un elemento crucial que contribuye a su buen funcionamiento. Cabe mencionar, no obstante, que la comunidad científica está buscando mecanismos de consenso alternativos que reporten similar seguridad sin un tercero de confianza, pero sin el consumo desperdiciado de energía. Hasta la fecha, ninguno de los mecanismos de consenso alternativos propuestos ha mostrado la fiabilidad del concepto de «prueba de trabajo» (llamado *proof-of-work,* en inglés) del Bitcóin.

IV. ¿ES EL BITCÓIN ÚTIL COMO MONEDA?

El Bitcóin se creó con la pretensión de constituir una nueva moneda. Pero ¿es realmente útil como moneda? La función crucial del dinero es servir como medio de pago. Hay muchas condiciones que un medio de pago debe cumplir para ser útil (20). Una es la de mantener su valor de una transacción a la siguiente. Si una «moneda» experimenta hiperinflación o alta volatilidad en su valor, no cumple realmente el requisito para ser un medio de pago útil.

Si comprar hoy una bicicleta cuesta 100 dólares, pero mañana cuesta 1.000 dólares y pasado mañana solo 20 dólares, el comercio con ella será menos apetecible. A los compradores les preocupará haber pagado en exceso, y a los comerciantes le preocupará que para cuando utilicen el dinero que reciban, su poder adquisitivo habrá caído de forma significativa. Una solución sería elevar el precio, pero eso desincentivaría a los compradores. En muchos países, los precios de los bienes y servicios fluctúan a lo largo del tiempo (habitualmente debido a la inflación), pero son relativamente estables de un día para otro. ¿Qué ocurre con los bitcoines? El gráfico 2 muestra un día típico en la cotización del Bitcóin. La diferencia entre el precio más bajo (unos 14.336 dólares) y el más alto (unos 18.353 dólares) supone aproximadamente un i28 por 100! Evidentemente, hay muchos días en los que el precio del Bitcóin no registra una variación tan drástica como la del gráfico 2, aunque hay unanimidad en que su precio es muy inestable. Esto puede desanimar a mucha gente a utilizarlo como medio de pago.

GRÁFICO 2
PRECIO DEL BITCÓIN (8 DE DICIEMBRE DE 2017)

Fuente: coinmarketcap.com

Otra razón es que, por ahora, utilizar bitcoines no es tan fácil como usar una tarjeta de crédito o los sistemas de pago instalados en los teléfonos móviles. Además, los usuarios potenciales afirman a menudo que los métodos de pago existentes satisfacen sus necesidades, y que no encuentran ningún motivo para adoptar uno nuevo (21).

También existe una razón técnica que podría limitar la adopción generalizada del Bitcóin. Recuérdese que en el Bitcóin las transacciones se procesan en bloques, a una velocidad de un bloque cada diez minutos. Por la forma en que está diseñado, un bloque en la cadena no puede superar un determinado tamaño, lo que limita seriamente el número de transacciones que pueden procesarse por la red de Bitcóin: como máximo siete transacciones por segundo. En comparación, VISA procesa de media miles de transacciones por segundo, pudiendo llegar a asumir hasta 56.000 transacciones por segundo (lo que equivale a casi 15.000 millones de transacciones al día!) (22).

En 2017, en múltiples ocasiones, la demanda de transacciones en Bitcóin superó la capacidad del sistema. En tales casos, el procesamiento de transacciones puede demorarse significativamente. Los usuarios pueden lograr que sus transacciones se procesen e incluyan en la cadena con mayor rapidez ofreciendo mayores comisiones a los mineros. De ese modo, hacia finales de 2017, se llegaron a pagar comisiones Bitcóin de hasta 30 dólares por transacción (23). En el caso de la mayoría de transacciones, esa cifra supera la que se cobra por pagar con tarjeta de crédito.

No obstante, hay ciertos casos en que la gente puede preferir utilizar Bitcóin en lugar de las alternativas disponibles en el tráfico comercial. Para ellos, la ventaja que únicamente el Bitcóin les confiere supera el riesgo de la volatilidad en su valor, la incomodidad de la interfaz y el coste de unas mayores comisiones. El tráfico ilegal (drogas, armas), el juego o la evasión fiscal fueron las primeras áreas en las que asistimos a un uso más frecuente de bitcoines. El relativo anonimato del Bitcóin y su velocidad lo hacen atractivo a los ojos de las personas involucradas en dichas actividades (24).

Hay algunos nichos de actividad legal que utilizan el Bitcóin, como la aviación privada. En ellos, la relativa privacidad, unida a la elevada cuantía de las transacciones, hacen al Bitcóin atractivo tanto para los comerciantes como para los compradores: los compradores consiguen más privacidad y no están constreñidos por límites de crédito en las tarjetas; los comerciantes reciben el dinero más rápido que a través de la tarjetas de crédito o de una transferencia bancaria, y se ahorran las comisiones que cobran los emisores de las tarjetas de crédito. Obsérvese que en el caso de una transacción de varios miles de dólares, la comisión de la tarjeta de crédito puede superar los 30 dólares; no es así para los comerciantes que realizan un gran número de transacciones individuales de pequeña cuantía. Esta asimetría procede del hecho interesante de que las comisiones de las tarjetas de crédito se basan en el valor de las transacciones, pero las comisiones Bitcóin se basan solamente en la urgencia del usuario.

La privacidad relativa y la naturaleza descentralizada de Bitcóin constituyen características útiles para los habitantes de países sujetos a férreos controles de cambios o riesgo de injerencia gubernamental en las cuentas bancarias; p. ej., casos en los que el gobierno limita la cantidad de reintegros diarios o semanales que pueden realizarse, o cuando el gobierno puede confiscar parte de los saldos depositados en las cuentas. Además, pese a la elevada volatilidad, Bitcóin puede ser preferido frente a monedas con muy alta inflación. Para los habitantes de países como Venezuela o Zimbabue, el Bitcóin puede resultar muy atractivo.

Ahora bien, y a pesar de los pocos nichos citados, tras ocho años de existencia, el Bitcóin no se ha convertido en un medio de pago popular. Alguien podría deducir que ello es el punto final de la historia del Bitcóin. Nada más lejos de la realidad.

V. ¿QUÉ SERÁ LO PRÓXIMO?

La «revolución del Bitcóin» no se detiene con la creación del Bitcóin. La historia no ha hecho más que comenzar. Bitcóin abrió la puerta a un amplio abanico de innovaciones e ideas, que pueden dividirse en dos categorías, criptomonedas y aplicaciones no monetarias.

1. Mejorando el Bitcóin: criptomonedas rivales

Cuando se habla de criptomonedas, casi todo el mundo piensa en Bitcóin, y la mayoría de la gente piensa que ésta es la única criptomoneda que existe. Pero no lo es. A finales de 2017, había más de mil criptomonedas diferentes cotizadas en los mercados digitales, es decir, estas criptomonedas podían comprarse o venderse a cambio de otras

monedas, como el dólar o el euro (si bien muchas de ellas solo son canjeables por bitcoines). La mayoría de estas monedas tienen un precio muy bajo, tanto que la capitalización total de mercado (esto es, el valor del total de monedas en circulación) asciende a tan solo unos miles de dólares. En comparación, la capitalización de mercado del Bitcóin a 31 de diciembre de 2017 rondaba los 240.000 millones de dólares! En dicha fecha existían algo menos de 40 criptomonedas con una capitalización de mercado superior a 1.000 millones de dólares cada una. Las principales criptomonedas por capitalización, al margen de Bitcóin, son ripple, ethereum y Bitcóin Cash. Al igual que el Bitcóin, estas criptomonedas son muy volátiles. Por ejemplo, litecoin, otra criptomoneda, tenía una capitalización cercana a los 20.000 millones de dólares el 19 de diciembre de 2017, pero dos semanas más tarde su valor descendió hasta casi 14.000 millones de dólares.

¿Por qué existen tantas criptomonedas? Hay varias razones. Una es obvia: la esperanza de hacer fortuna de forma rápida. Dado el vertiginoso crecimiento del Bitcóin, hay quien cree que puede conseguir captar mucho dinero si crea o identifica dónde está el «nuevo Bitcóin». Por esta razón, muchas criptomonedas se limitaban a ser meras copias de Bitcóin. Bitcóin es un proyecto de código abierto. Cualquiera puede utilizarlo, con o sin cambios. Cualquiera puede lanzar al mercado una copia que imite a Bitcóin. Como era de imaginar, la mayoría de estas imitaciones no tuvieron éxito, y dejando de lado algunos esquemas especulativos que inflaron el precio para lucrarse a costa de los que vinieron detrás, consiguieron capitalizaciones de mercado muy escasas.

Sin embargo, la posibilidad de alterar el código abierto de Bitcóin dio lugar al desarrollo de criptomonedas con una motivación diferente: la de mejorar el Bitcóin.

Como se ha explicado en la sección cuarta, el Bitcóin presenta una serie de carencias. Por su diseño, puede procesar un máximo de siete transacciones por segundo. Por tanto, si alguna criptomoneda llegara un día a convertirse en un medio de pago utilizado popularmente, no sería el Bitcóin tal como lo conocemos hoy. Existen dos formas posibles de arreglar esto. La primera es que el Bitcóin evolucione y su *software* se actualice de manera que permita un mayor flujo de transacciones. El problema es que ahí radica precisamente la innovación de Bitcóin; en su carácter descentralizado. No existe una estructura de gobernanza en la que una autoridad o un comité tengan la potestad de implementar cambios en el protocolo Bitcóin. Para cualquier modificación del protocolo Bitcóin se requiere la opinión favorable de una mayoría abrumadora de los mineros, o incluso la unanimidad. Esto resulta muy difícil de llevar a la práctica. En verano de 2017 un grupo de mineros y usuarios de Bitcóin propusieron un cambio. Para su adopción se necesitaba que un 95 por 100 de los mineros lo aceptase. Dicha mayoría no fue alcanzada, con lo que el protocolo Bitcóin permaneció inalterado. Ahora bien, un porcentaje significativo de mineros implementaron el cambio propuesto, lo que dio origen a una nueva versión de Bitcóin que denominaron *Bitcóin Cash*. Existe en paralelo con Bitcóin. Y esta convivencia paralela apunta a la segunda manera en que una criptomoneda podría llegar a convertirse en un medio de pago de uso generalizado; que surja otra criptomoneda, mejorada, que sea capaz de procesar mayores volúmenes de transacciones y desbanque en adopción a Bitcóin, convirtiéndose en dominante en el mercado.

Otro problema del Bitcóin es que el número total de monedas que se pueden minar al cabo del tiempo es fijo. A largo plazo, esto creará dinámicas deflacionistas, es decir, en lugar de que los precios suban (inflación), los precios disminuirán. Una bajada puntual y no recurrente de los precios, como en el *black friday,* es bien recibida por los consumidores, pero no lo es si dicho descenso es persistente. Para demostrarlo, imaginemos que tenemos que pagar una hipoteca con una cuota de, digamos, 1.000 dólares al mes. Si los precios caen durante un período prolongado, también lo harán los salarios, mientras que la cuantía de la cuota mensual seguirá siendo la misma. Esto significa que la parte de los ingresos destinada al pago de la hipoteca aumenta. Lo mismo es aplicable a aquellas empresas que contrajeron un préstamo para financiar sus inversiones. Otro efecto de la deflación es que los consumidores aplazan todo lo posible sus decisiones de compra de bienes duraderos (como una lavadora), especialmente cuando son productos costosos. Si todo el mundo se comporta de la misma forma, la actividad económica se frena.

Muchas de las criptomonedas creadas después del Bitcóin tienden a corregir uno o varios de los «fallos» de ésta. Por ejemplo, litecoin es una criptomoneda que busca procesar transaccio-

nes más rápido que el Bitcóin. Con litecoin, el tiempo medio que se tarda en añadir un bloque a la cadena de litecoin es de solo 2,5 minutos (frente a los diez minutos de Bitcóin), y los bloques están diseñados de tal manera que litecoin puede procesar hasta 56 transacciones por segundo (frente a solo siete por segundo en el caso de Bitcóin). Litecoin utiliza también diferentes algoritmos para los problemas numéricos que los mineros deben resolver, algo originalmente encaminado a reducir la cantidad de energía utilizada en el proceso de minado (véase, por ejemplo, Gandal y Halaburda, 2016). Muchas de las criptomonedas existentes (¡y las de próxima aparición!) comparten la misma motivación que inspiró la creación de litecoin: mejorar el diseño de Bitcóin. Y a pesar de la popularidad actualmente incontestable del Bitcóin, es posible que la criptomoneda del futuro sea una de las competidoras.

2. Contratos inteligentes: el Ethereum y más allá

Un salto de gigante en el ámbito de las criptomonedas y de la cadena de bloques fue la creación de la *plataforma Ethereum*. El Ethereum fue propuesto a finales de 2013 por un joven programador, Vitalik Buterin. El desarrollo del Ethereum comenzó poco tiempo después (financiado a través de una *crowd-sale* en el verano de 2014) y su lanzamiento oficial se produjo el 30 de julio de 2015.

El sistema Ethereum es similar al Bitcóin en muchos aspectos: tiene una cadena de bloques y mineros, así como una criptomoneda, denominada ether. Ofrece una nueva funcionalidad respecto al Bitcóin y a otras criptomonedas al incorporar los contratos inteligentes.

Por «contrato inteligente» (*smart contract*) se entiende un conjunto de instrucciones que se ejecutan automáticamente cuando se cumplen ciertas condiciones, impuestas por el usuario. Un ejemplo muy sencillo de contrato inteligente sería el siguiente. Supongamos dos usuarios, Alicia y Bob: Alicia vende su casa a Bob. Bob puede pagar a Alicia por medio de la red Ethereum, pero añade en su transacción el siguiente contrato inteligente: Alicia recibirá los ether correspondientes a la transacción solo si, antes de una determinada fecha, el Registro de la Propiedad (de cuyo mantenimiento se encargan las autoridades locales) indica que el inmueble ha pasado a pertenecer a Bob. En este ejemplo, el contrato inteligente funcionaría así: el programa (es decir, el contrato inteligente) comprueba periódicamente si en el Registro de la Propiedad Bob consta como propietario. Si es así, Alicia recibe los ether que Bob envió en pago. Por supuesto, tal contrato inteligente solo es posible si el Registro de la Propiedad tiene habilitada la posibilidad de acceder a él por vía remota a través de un programa.

Otra aplicación potencial de los contratos inteligentes es el pago de la tasa de demora en la industria naval. Cuando un contenedor llega a su puerto de destino, la llegada es anotada por las autoridades portuarias en una base de datos. Esto puede activar la ejecución de un contrato inteligente que finalice el pago entre el vendedor y el comprador, lo que incluiría la posible penalización a pagar por el vendedor (o la compañía transportista) en caso de que el contenedor llegue con retraso.

Un *contrato inteligente* puede parecer una expresión ingeniosa, pero el concepto no nació con el Ethereum. Los pagos automáticos para domiciliar el pago de nuestros recibos, alquileres o hipotecas en el banco son, de hecho, contratos inteligentes. La ventaja de los contratos inteligentes de Ethereum respecto a los que ofrecen nuestros bancos es que pueden diseñarse de la manera que queramos. El Bitcóin permitió almacenar contratos inteligentes rudimentarios en la cadena de bloques. Pero solo con el Ethereum fue posible que dos partes incluyeran en su cadena cualquier contrato inteligente susceptible de ser programado. Esto se traduce en mayor flexibilidad y funcionalidad.

Por supuesto, el atractivo de los contratos inteligentes depende de la capacidad de confirmar independientemente vía terceros no vinculados que determinadas condiciones se han cumplido. En el ejemplo anterior de Alicia y Bob, para que los contratos inteligentes funcionen, las escrituras de propiedad han de estar en soporte digital y estar abiertas a programas que quieran analizarlas. Para los envíos de mercancías por mar, también se precisa que las autoridades portuarias y los transportistas registren sus actuaciones en bases de datos accesibles de forma remota por terceros. Los contratos inteligentes como los que hemos descrito no son todavía ubicuos porque la infraestructura necesaria para ellos está aún en una fase incipiente (*trackers* para los envíos, bases de datos legales accesibles de forma remota, etcétera).

En su fundamento, dichos contratos inteligentes no necesitan de una solución de cadena de bloques como el Ethereum: una simple base de datos centra-

lizada también funcionaría. No obstante, la posibilidad de crear contratos inteligentes a medida para muchas personas es un factor decisivo que podría reportar significativos ahorros de costes.

3. Una funcionalidad alternativa de las criptomonedas: las *initial coin offerings*

La actividad de mercado, así como el análisis académico, indican que muchas personas están adquiriendo bitcoines y otras criptomonedas exclusivamente con fines de inversión, y no porque esperen que un día llegarán a utilizarse de manera generalizada. No hay mejor prueba del potencial de las criptomonedas como inversión que la proliferación de ICO, o *initial coin offerings,* desde 2016.

La semejanza del acrónimo «ICO» con el de «IPO» (oferta pública inicial de acciones cuando una empresa sale a cotizar en Bolsa) no es casual. La IPO es una forma que tienen las empresas de captar dinero del público aumentando su capital con la venta de participaciones, o acciones, de la compañía. Tras la venta inicial, las acciones cotizan en mercados como Nasdaq. Los reguladores establecieron unos estrictos requisitos que cualquier compañía que quisiera vender sus acciones al público había de cumplir para asegurarse de que, una vez captado el dinero, no desapareciera y dejara a los inversores en la estacada. Así pues, tradicionalmente, solo las empresas que son lo suficientemente grandes y estables han sido capaces de cumplir esta carga regulatoria y lanzar una IPO. Asimismo, salir a Bolsa suele verse como un hito para una compañía. Pero debido a los requisitos, la preparación de la IPO es una tarea costosa, ardua y arriesgada. No todas las que inician el proceso reciben eventualmente la autorización para lanzar la IPO.

Las criptomonedas (las «monedas») se convirtieron en una alternativa atractiva para algunas compañías, al eliminar los trámites administrativos y los requerimientos impuestos a una empresa que salía a Bolsa. Una ICO es de hecho como un *crowdfunding,* y en esto se asemeja también a una IPO. Alguien propone un proyecto y solicita la contribución de los individuos o inversores. En el caso de una IPO, los contribuyentes obtienen acciones de la compañía. En el *crowdfunding*, el caso típico consiste en obtener un objeto con algún descuento o ser uno de los primeros en recibirlo. En el caso de una ICO, los contribuyentes obtienen *tokens*. Ahora bien, no está claro qué representa un *token*.

En ocasiones, la ICO es para el lanzamiento de una nueva criptomoneda. En tal caso, los *tokens* representan las nuevas monedas. Es decir, un contribuyente al proyecto recibe *tokens* que, en una fecha posterior, son convertidos en monedas de la nueva criptomoneda. Esto es, por ejemplo, lo que ocurrió con el Ethereum.

Es tentador ver los *tokens* de las ICO recibidos por un contribuyente como acciones de la compañía. Pero, en la mayoría de los casos, no lo son. No hay reglas ni supervisión acerca de qué representan los *tokens* o qué valor otorgan a su propietario. Invertir en una ICO es, por tanto, arriesgado pues no hay garantías contractuales de que un inversor acabará recibiendo acciones de la compañía, menos aún dividendos.

4. Mirando al futuro: aplicaciones de la cadena de bloques

Para muchas personas, la originalidad del Bitcóin no solo consiste en ofrecer un sistema descentralizado de dinero. Ven potencial en el concepto de una cadena de bloques —y en cómo se mantiene— para usos diferentes de una criptomoneda. Después de todo, según parece, una cadena de bloques no es más que una base de datos.

Técnicamente, la cadena de bloques de Bitcóin es una base de datos distribuida y no sujeta a permisos. ¿Qué significa esto? *Distribuida* significa que múltiples miembros de la red pueden efectuar cambios en la base de datos. El reto en tal supuesto es asegurar la consistencia de dicha base de datos entre los diferentes miembros de la red. Las bases de datos distribuidas vienen usándose y aplicándose desde hace tres décadas. Sin embargo, el diseño de todas las que precedieron al Bitcóin implicaban a un tercero que gestionaba el acceso de los miembros de la red a la base de datos a menudo, también ejercía de árbitro en caso de conflicto; eran bases de datos distribuidas sujetas a permisos. El Bitcóin, en cambio, es una base de datos distribuida *no sujeta a permisos*. Esto significa que cualquiera puede modificarla (es decir, ser minero en el caso del Bitcóin): no hace falta el permiso de ningún tercero para ello (25).

Satoshi Nakamoto no inventó el concepto de base de datos distribuida y no sujeta a permisos. La comunidad criptográfica llevaba trabajando en ese concepto desde mediados de la década de los años ochenta del siglo pasado. Hubo varios intentos

infructuosos. La aportación de Satoshi Nakamoto al diseñar el Bitcóin estribó en ir más allá de soluciones criptográficas y basarse ampliamente en un sistema de incentivos económicos para conseguir la consistencia de la base de datos. Esto condujo a un esquema de incentivos para los mineros articulado en torno a una estructura competitiva basada en la prueba de trabajo y en una recompensa. Un factor crucial para la consistencia de la base de datos es la estructura *append-only*, es decir, que solo se puedan añadir registros nuevos (los cuales han de ser compatibles con los ya existentes) a la base de datos, configurando la denominada cadena de bloques. Puesto que la base de datos no se diseñó para permitir reescribir entradas anteriores, todo intento de bifurcar la cadena por un atacante exige crear una base de datos alternativa (es decir, una cadena alternativa) y generar condiciones por las que la base de datos alternativa pueda ser aceptada en sustitución de la original (es decir, construir una cadena más larga). Un inconveniente es que la estructura *append-only* tiene una contrapartida: la menor velocidad a la hora de consultar la base de datos. La mayoría de las bases de datos que utilizan los gobiernos, nuestros bancos y otras corporaciones (denominadas *bases de datos relacionales*) son más complejas, pero más rápidas de consultar.

No tuvo que pasar mucho tiempo para que la gente vislumbrase otros usos posibles de la «tecnología *blockchain*» además del de mantener una moneda digital. Implementar una base de datos distribuida y no sujeta a permisos que fuera fiable podría eliminar la necesidad de terceros que comprueben y verifiquen la veracidad de los datos. Por ejemplo, si queremos comprar una casa, tendremos que comprobar que el vendedor es realmente el propietario. Igualmente, el vendedor querrá comprobar que contamos con suficientes fondos para pagarla. Todas esas operaciones implican abogados, intermediarios y/o notarios. Muchas personas creen que una tecnología *blockchain* (que hiciese accesibles todos los datos necesarios en tales transacciones) nos permitiría prescindir de dichos intermediarios. En el sector financiero, los bancos y los inversores creen que si las operaciones con valores (acciones, bonos, derivados, etc.) se registrasen en una base de datos distribuida, sería más fácil realizar el seguimiento de la titularidad y se facilitarían las liquidaciones (la transferencia del activo del vendedor al comprador).

Ahora bien, las aplicaciones potenciales de la «tecnología *blockchain*» no siguen exactamente el patrón del Bitcóin. Muchas aplicaciones del *blockchain* en fase de desarrollo consideran una base de datos *privada* (no todos pueden descargar y examinar los datos) y *sujeta a permisos* (la capacidad de modificar o introducir nuevos datos la otorga un tercero). No hay una definición comúnmente aceptada de *blockchain,* aunque las características sobre las que la mayoría coinciden son su carácter *distribuido y append-only.* Esto representa una diferencia respecto a la idea inicial de Bitcóin que condujo a una base de datos distribuida y *no sujeta a permisos*.

Un ejemplo de dicha interpretación amplia de la tecnología de *blockchain* es la e-ciudadanía implementada en Estonia. En Estonia, el ejercicio del voto, las transmisiones de inmuebles, la gestión de los impuestos, la banca, las relaciones con la escuela o los datos sanitarios se vehiculan ahora a través de Internet. Los datos no están almacenados de forma centralizada, sino en miles de servidores, y la tecnología detrás de la plataforma (denominada X-Road) se declara deudora del diseño del *blockchain* (26). Nótese que, en este caso, nos separamos de la «filosofía Bitcóin» porque el *blockchain* estonio está controlado por el gobierno.

VI. CONCLUSIONES

Casi diez años después de su creación, el Bitcóin ha logrado convertirse en un término común para los ciudadanos de a pie. Cada día, miles de personas compran o venden bitcoines y otras criptomonedas, y hay incluso quienes utilizan bitcoines para lo que fueron inventados, como medio de pago de bienes y servicios. No existe ninguna duda de que el diseño de Bitcóin es un exitoso intento de crear un sistema de dinero digital *descentralizado*. Algo más incierto, por el momento, es si los bitcoines pueden afirmar su estatus como moneda. Debido a una serie de limitaciones inherentes, el Bitcóin no resulta adecuado para su uso generalizado. Pero quizá otras criptomonedas sí lo sean.

La contribución del Bitcóin va más allá de ser una criptomoneda. La pasión en torno a las propiedades del *blockchain* asociado al diseño tecnológico del Bitcóin ha alentado el debate sobre su uso en una amplia gama de aplicaciones. En efecto, ha puesto el foco en los contratos inteligentes y las bases de datos distribuidas y propiciado

algunos usos innovadores. Si lo pensamos bien, la mayoría de los desarrollos y aplicaciones propuestas no son nuevas. Los conceptos de bases de datos distribuidas y contratos inteligentes existían mucho antes del Bitcóin o del Ethereum.

Para sus partidarios, las soluciones basadas en el *blockchain* son infinitas. Proyectos actuales que se definen inspirados en el *blockchain* van desde sistemas de votación (*Soverign*) o de gestión de carteras de renta variable (*Chain*, lanzado por Nasdaq) hasta el registro de dominios de Internet (*Namecoin*) o el almacenamiento de archivos (*Storj*). Pero lo cierto es que, a día de hoy, sigue sin aparecer la *killer application* para esta tecnología que promueva su adopción masiva.

Así pues, ¿es el Bitcóin verdaderamente una revolución? Podemos afirmar sin temor que sí. Cabe discutir hasta qué punto el Bitcóin aportó o no grandes dosis de innovación (pues la mayoría de los conceptos ya existían), pero de lo que no hay duda es de que la popularidad que se han forjado el Bitcóin y el *blockchain* han impulsado el debate y el desarrollo de soluciones descentralizadas y automatizadas.

NOTAS

(*) Agradecemos a Debbie Haeringer, Lukasz Pomorski, Meredith Stevens y Larry White sus valiosos comentarios y sugerencias.

(**) Las opiniones presentadas corresponden al autor y no coinciden necesariamente con la postura oficial de Bank of Canada.

(1) El artículo está disponible aquí: https://bitco.in/pdf/bitcoin.pdf. A día de hoy, la verdadera identidad de Satoshi Nakamoto sigue siendo desconocida.

(2) En tiempos modernos, los cigarrillos utilizados en los campos de detención por los prisioneros de guerra guardan similitud con los ejemplos de dinero que no requieren un tercero de confianza (véase Radford, 1945).

(3) Utilizamos el término Bitcóin con mayúscula para referirnos al sistema. Como la mayoría de monedas, el Bitcóin admite fracciones decimales. La unidad más pequeña es el satoshi, y representa una cienmillonésima de Bitcóin, es decir, un satoshi equivale a 0,00000001 bitcoines.

(4) Las «monedas de Bitcóin» que se pueden adquirir en webs como eBay o Amazon no son bitcoines, sino meras piezas de metal en las que aparece la inscripción «Bitcóin».

(5) Esta dirección de Bitcóin es una de las primeras direcciones de Bitcóin que se generaron y se cree que pertenece al propio Nakamoto.

(6) Bitcóin respalda diferentes maneras de codificar (es decir, reformular) la clave privada en una cadena de caracteres.

(7) Y cada vez más grande: a finales de 2017 el tamaño de la cadena de Bitcóin sumaba casi 150 gigabytes.

(8) Es por esto por lo que decimos que la dirección de Bitcóin mostrada más arriba *se cree* que pertenece a Satoshi Nakamoto.

(9) Las estimaciones oscilan entre 10.000 (bitnodes.earn.com) y 30.000. Véase también https://en.bitcoin.it/wiki/Clearing_Up_Misconceptions_About_Full_Nodes

(10) http://fortune.com/2017/11/25/lost-bitcoines/

(11) Algunas de las webs más populares, aunque no las únicas, son coinbase.com, bitstamp.com o blockchain.info.

(12) La red del Bitcóin es simplemente una red de computadoras conectadas entre sí a través de Internet.

(13) Decimos que «probablemente es el propietario» porque podría ser un ladrón que ha robado el monedero a alguien.

(14) Para el lector interesado: el problema está basado en un algoritmo denominado *hashing*, que es bien conocido y se utiliza comúnmente en criptografía. Véase https://en.wikipedia.org/wiki/Cryptographic hash function

(15) Véase, p. ej., https://digiconomist.net/bitcoin-energy-consumption; https://arstechnica.com/tech-policy/2017/12/bitcoines-insane-energy-consumption-explained/

(16) Una alternativa sería sustituir la transacción por otra en la que Zoe se enviase sus bitcoines a ella misma (p. ej., a otra dirección suya) en lugar de a la dirección del vendedor de la bicicleta. La mecánica sería la misma. Sin embargo, no puede crear una transacción en la que el vendedor le envíe los bitcoines de vuelta a ella. Para ello, necesitaría conocer la clave privada del vendedor, y hacerlo antes de que el vendedor se gaste sus bitcoines.

(17) Transmitir datos a través de Internet puede ser rápido, pero no *instantáneo* porque la velocidad de transmisión de datos está condicionada por la velocidad de la luz. Por ejemplo, Nueva York y Tokio están a algo más de 10.000 km de distancia, de modo que es *imposible* tardar menos de sesenta y siete milisegundos en enviar datos de una ciudad a otra. Si consigues transmitir datos más rápido, habrás conseguido refutar a Einstein.

(18) Los bloques de Alicia y de Bob también pueden tener algunas transacciones en común. Si Bob quiere crear un bloque después del bloque de Alicia, necesitará reconstruir primero el grupo de transacciones que quiere procesar, eliminando de él las transacciones ya procesadas por Alicia.

(19) Algunos análisis detallados muestran que en torno al 30 por 100 o 40 por 100 es, de hecho, suficiente para tener una probabilidad muy elevada de construir una cadena competidora más larga. Véase, p. ej., Kiayias *et al.* (2016).

(20) A menudo los economistas se refieren a una conocida definición del dinero como medio de pago, unidad de cuenta y depósito de valor. Estos dos últimos aspectos del dinero son imprescindibles para que, además, pueda cumplir la primera función. Pero hay otras condiciones, por ejemplo, la de ser razonablemente divisible. Cuando el dinero se representa en forma de objetos físicos, también debe ser uniforme, duradero, fácil de transportar, etc.

(21) Véase, p. ej., los resultados de la encuesta de Henry y Nicholls (2018).

(22) https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

(23) Véase, p. ej., https://news.bitcoin.com/miami-bitcoin-conference-stops-accepting-bitcoin-due-to-fees-and-congestion/

(24) Lleva solo unas horas enviar bitcoines a la otra punta del mundo, mientras que las transferencias bancarias internacionales tardan varios días. Servicios como Western Union son veloces, pero las comisiones que

cobran pueden ser superiores y en algunos países no preservan tanto el anonimato para cantidades grandes como Bitcóin.

(25) La obligación de resolver un problema difícil como paso previo para añadir bloques a la cadena no es incompatible con la no sujeción a permisos, ya que cualquiera que lo desee puede ser minero.

(26) Existe una copia de respaldo del sistema en servidores en Luxemburgo, como medida de seguridad frente a averías o a una invasión por parte de Rusia.

BIBLIOGRAFÍA

ANDROULAKI, E; KARAME, G. O.; ROESCHLIN, M.; SCHERER, T., y S. CAPKUN (2013), «Evaluating user privacy in bitcoin», *International Conference on Financial Cryptography and Data Security*, Springer, 34.

FERGUSON, N. (2008), *The ascent of money: A financial history of the world*, Penguin.

GANDAL, N., y H. HALABURDA (2016), «Can we predict the winner in a market with network effects? Competition in cryptocurrency market», *Games*, 7: 16.

HALABURDA, H., y M. SARVARY (2016), *Beyond bitcoin. The economics of digital currencies*, Springer.

HENRY, C.; HUYNH, S., K. P., y G. NICHOLLS (2018), «Bitcoin awareness and usage in Canada», *Journal of Digital Banking* (en prensa).

KIAYIAS, A.; KOUTSOUPIAS, E.; KYROPOULOU, M., e Y. TSELEKOUNIS (2016), «Blockchain mining games», in *Proceedings of the 2016 ACM Conference on Economics and Computation*, ACM: 365-382.

NAKAMOTO, S. (2008), «*Bitcoin: A peer-to-peer electronic cash system*». *www.bitcoin.org, https://bitcoin.org/bitcoin.pdf*

RADFORD, R. A. (1945), «The economic organisation of a POW camp», *Economica*, 12: 189-201.

ROBERTS, J. J., y N. RAPP (2017), «Exclusive: Nearly 4 million bitcoines lost forever», *Fortune*, November 25, http://fortune.com/2017/11/25/lost-bitcoines/

URQUHART, A. (2016), «The inefficiency of bitcoin», *Economics Letters*, 148: 80-82.