BITCOIN: ¿UNA SOLUCIÓN PARA LOS SISTEMAS DE PAGO O UNA SOLUCIÓN EN BUSCA DE PROBLEMA?

2019

Carlos Conesa

Documentos Ocasionales
N.º 1901

BANCO DE ESPAÑA
Eurosistema

BITCOIN: ¿UNA SOLUCIÓN PARA LOS SISTEMAS DE PAGO O UNA SOLUCIÓN EN BUSCA DE PROBLEMA?

BITCOIN: ¿UNA SOLUCIÓN PARA LOS SISTEMAS DE PAGO O UNA SOLUCIÓN EN BUSCA DE PROBLEMA?

Carlos Conesa (*)

BANCO DE ESPAÑA

(*) El autor agradece los comentarios de Juan Ayuso, José Manuel Marqués, Sergio Gorjón y José Luis Romero.

Documentos Ocasionales. N.º 1901
2019

ISSN: 1696-2230 (edición electrónica)

Resumen

En octubre de 2008 se publicó un misterioso artículo bajo el seudónimo de Satoshi Nakamoto: «Bitcoin: a peer-to-peer electronic cash system». Meses después, a principios de 2009, Bitcoin comenzó a operar sin generar apenas atención. Desde entonces hasta hoy, el esquema ha acumulado más de medio millón de eslabones en su cadena de bloques o *blockchain,* que recogen más de 300 millones de operaciones. Teniendo en cuenta la repercusión mediática que ha generado *Bitcoin,* parece conveniente explicar con un cierto grado de detalle su funcionamiento y limitaciones. Este documento revisa los objetivos que se perseguían con la creación de Bitcoin y su funcionamiento básico, analiza sus ventajas e inconvenientes, y discute su utilidad como mecanismo de intercambio.

Palabras clave: *blockchain,* función *hash, bitcoin,* criptoactivos, criptografía, innovación, tecnología.

Códigos JEL: O31, O33.

Abstract

In October 2008 a mysterious article was published under the pseudonym Satoshi Nakamoto: “Bitcoin: a peer-to-peer electronic cash system”. Bitcoin’s entry into operation some months later in early 2009 barely caused a ripple. Since then, the scheme has accumulated more than half a million blocks in its blockchain and they include more than 300 million transactions. In view of the media impact of Bitcoin, it is worth explaining in some detail how Bitcoin works and what its limitations are. This article reviews the aims and basic functioning of Bitcoin, analyses its strengths and weaknesses, and discusses its usefulness as an exchange mechanism.

Keywords: blockchain, hash function, bitcoin, cryptoassets, cryptography, innovation, technology.

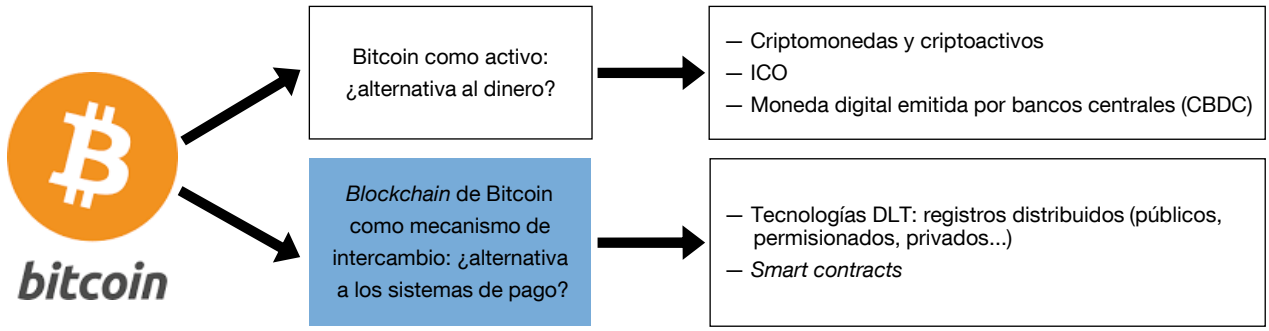
JEL classification: O31, O33.

ÍNDICE

1 Introducción

Bitcoin ha generado un creciente interés en los últimos años, y, además, el debate que provocó se ha ramificado. Inicialmente, la discusión sobre Bitcoin se bifurcó en dos áreas. Por un lado, el estudio de los *bitcoins* como activo y la posibilidad de que pudieran ser una alternativa al dinero fiduciario. Por otro, el análisis del *blockchain* como mecanismo de intercambio y sus posibilidades como sistema de pago o de compensación y liquidación de valores u otros activos. Mientras tanto, la cotización del *bitcoin* ha experimentado fuertes altibajos, pasando de cero a rozar los 20.000 USD por *bitcoin.* En la actualidad (diciembre de 2018), su precio está en torno a los 3.500 USD por *bitcoin.* Como se muestra en el esquema 1, el debate previamente expuesto se ha complicado todavía más. El presente documento se centra en el análisis de Bitcoin como mecanismo de intercambio, concretamente en sus fortalezas y debilidades como alternativa a los sistemas de pago tradicionales.

LA EVOLUCIÓN DEL DEBATE: DE BITCOIN A CRIPTOACTIVOS Y TECNOLOGÍAS DE REGISTROS DISTRIBUIDOS (DLT) ESQUEMA 1



FUENTE: Elaboración propia.

2 ¿Por qué Bitcoin funciona como funciona?

En este documento se ofrece una visión del funcionamiento del mecanismo de intercambio de Bitcoin algo más detallada que la que suele aparecer en resúmenes similares. Aunque se evita el exceso de detalles técnicos, es conveniente conocer algunos conceptos básicos de criptografía (funciones *hash* y criptografía asimétrica). Estos conceptos básicos se recogen en el recuadro 1. Además, se presenta Bitcoin de forma diferente a la habitual. En vez de explicar sin más el funcionamiento del esquema, se utilizará un enfoque iterativo, mediante el cual se construirá un modelo de criptomoneda similar a Bitcoin a partir de cero[1]. Este procedimiento es más lento, pero la resolución de los problemas que irán apareciendo será útil para explicar por qué Bitcoin funciona como lo hace y no de otra manera.

1 Las secciones 2.1 y 2.2, incluyendo el enfoque iterativo y las sucesivas modificaciones del protocolo de prueba, están tomadas de Nielsen (2013), con algunas modificaciones. La principal modificación es la asimilación de las direcciones de Bitcoin a números de cuenta y no a referencias o números de serie de las monedas, que podrían cuestionar su fungibilidad.

CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA ASIMÉTRICA Y FUNCIONES *HASH* — RECUADRO 1

En este recuadro se recogen algunos conceptos básicos sobre criptografía relacionados con el funcionamiento de Bitcoin descrito en el documento. Las explicaciones tienen carácter divulgativo: no pretenden ser precisas, sino aportar el conocimiento básico para comprender el funcionamiento de Bitcoin.

Se puede definir criptografía o cifrado como un procedimiento que utiliza un algoritmo con una clave (clave de cifrado) y transforma un mensaje de tal modo que sea incomprensible para toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

En su forma clásica, la criptografía utiliza la misma clave para cifrar y descifrar mensajes, con lo que no resuelve totalmente el problema de seguridad. Los destinatarios del mensaje tienen que intercambiar bilateralmente la clave de cifrado, por lo que se exponen a que un tercero intercepte dicha clave y pueda así acceder a la información que intercambian. Además, el número de intercambios bilaterales de claves es inmanejable si el número de participantes que intercambian información es alto (véase esquema A).

En la actualidad se utiliza ampliamente una versión evolucionada denominada «criptografía asimétrica» o «de dos claves». En este caso, se generan dos claves relacionadas, una de las cuales se mantiene secreta (S) y la otra es pública (P). Estas dos claves se generan con programas específicos a partir de un número aleatorio y es prácticamente imposible deducir cuál es S a partir de P, y viceversa

Esquema A
CRIPTOGRAFÍA SIMÉTRICA

FUENTE: Elaboración propia.

(siempre y cuando el proceso de generación de las claves se haya realizado correctamente). La criptografía asimétrica se puede comparar con un candado con dos llaves: si se realiza una encriptación (cierre del candado) con S, solo se podrá desencriptar con P (apertura del candado), y viceversa (véase esquema B).

La criptografía asimétrica se suele combinar con una autoridad de certificación que verifica la identidad de una persona en el momento de generar y comunicarle su par de claves. Esa persona debe mantener su clave privada secreta, mientras que la clave pública es fácilmente accesible a todos los participantes.

La criptografía asimétrica permite asegurar la confidencialidad en las comunicaciones y también autenticar al emisor de un mensaje.

Confidencialidad: supongamos que una persona (Alicia) desea enviar un mensaje cifrado a otra (Bruno). Para ello, Alicia cifra el mensaje con la clave pública de Bruno, de forma que solo Bruno podrá descifrarlo con su clave privada. Nótese, que a diferencia de la criptografía clásica o simétrica, no hay necesidad de que Alicia y Bruno se intercambien previamente las claves de cifrado.

Autenticación o firma electrónica: supongamos que Alicia quiere probar que ella ha escrito un mensaje. Para ello, envía el mensaje a otra persona y adjunta una copia cifrada con su clave secreta del mismo mensaje. El receptor utiliza la clave pública de Alicia para descifrar el mensaje encriptado y lo compara con la información sin encriptar. Si son iguales, está claro que solo Alicia pudo haber realizado el envío.

Otra herramienta de utilidad para comprender el funcionamiento de Bitcoin es la **función *hash*.** Es una función criptográfica (H) que, dada una entrada x (cualquier texto o valor de longitud variable), devuelve una salida h (denominada *digest* o *hash)* de longitud fija (H(x) = h). La función *hash* que cumple las siguientes propiedades:

- Es «trivial», dado un *input* x, hallar su *hash* h.
- Es «imposible», dado h, hallar x (función no invertible).
- Es «imposible» modificar x sin cambiar h. Pequeños cambios en x devuelven *outputs* h completamente diferentes.
- Es «imposible» encontrar dos x que devuelvan el mismo h[1]

La función *hash* tiene múltiples utilidades:

Se puede utilizar para incrementar la **seguridad.** Un comerciante puede optar por almacenar los *hashes* de las contraseñas de sus clientes, en vez de las contraseñas en plano. De esta forma, cuando un usuario teclea su contraseña x, la empresa calcula el *hash* h (proceso trivial) y lo compara con el *hash* almacenado. Si coinciden, el usuario puede proceder con su compra. Si un *hacker* roba la información almacenada por la empresa, solo podría acceder a los *hashes* de las contraseñas de los usuarios, que no le permiten acceder a la contraseña (obtener x a partir de h es impracticable).

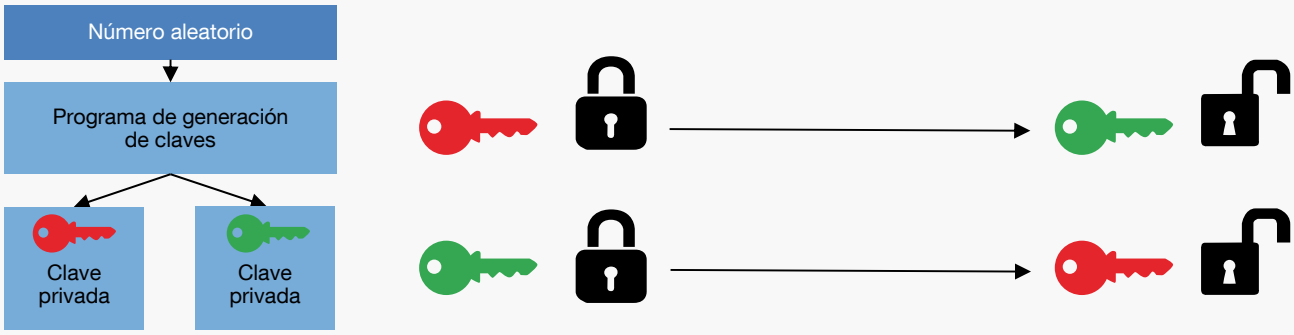
Se puede utilizar para **verificar la integridad de la información.** Para ello se compara el *hash* de un mensaje antes de enviarlo con el que genera en destino. Si se ha introducido alguna modificación, los *hashes* serán muy diferentes, y comparar dos *hashes* es muy sencillo, porque son de tamaño limitado.

También se puede usar como **resumen o «huella digital»** de un *input* muy extenso.

También se puede usar para **construir una prueba de trabajo,** de la que se hace un amplio uso en Bitcoin y que también tiene otros

1 Con «trivial» se indica que el consumo de recursos computacionales es extremadamente bajo. Con «imposible» se quiere indicar que el consumo de recursos computacionales que requeriría encontrar una solución hace impracticable el proceso. A título de ejemplo, si tenemos una función H que da un *hash* de 256 bits (como SHA-256, usada en Bitcoin), si se desea encontrar dos x que den el mismo h, habrá que hacer de media 2.128 intentos. En un ordenador que calcule 10.000 hashes por segundo, esto supone 1.027 años de trabajo [Nayaranan *et al.,* (2016)].

Esquema B
CRIPTOGRAFÍA ASIMÉTRICA



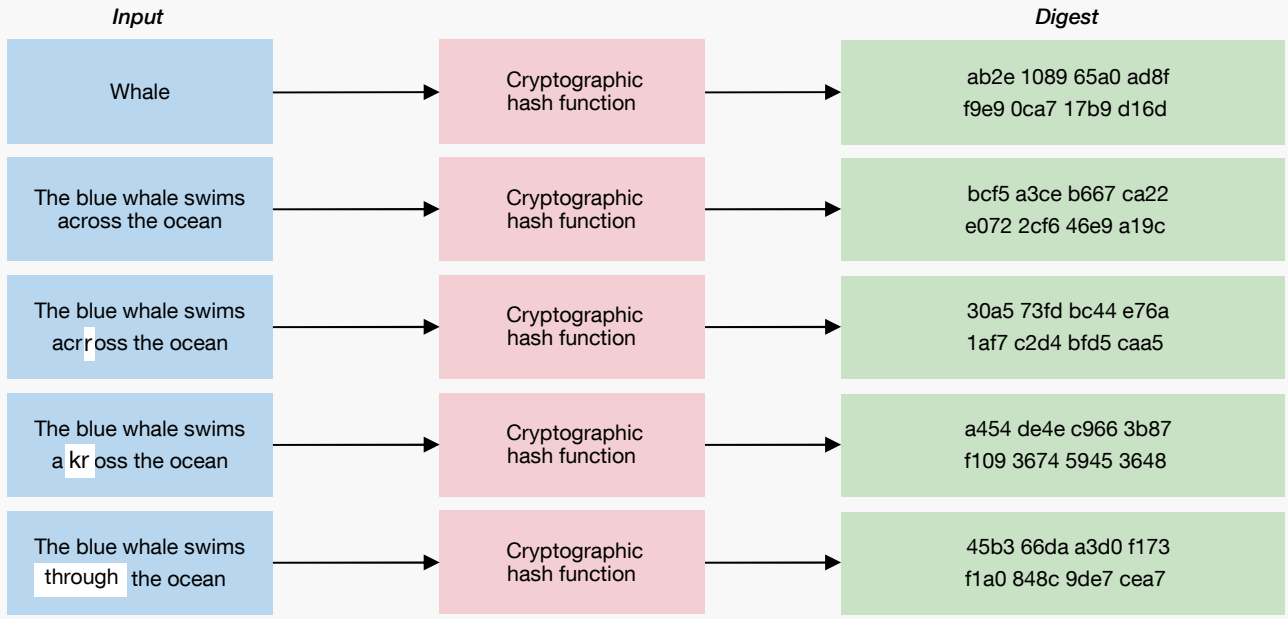
FUENTE: Elaboración propia.

usos, como dificultar los ataques de denegación de servicio. Imaginemos un comerciante que mantiene una página web de su comercio. Cada vez que un cliente accede a su web, desencadena una serie de peticiones (acceso al catálogo, pedidos, consultas) que el sistema informático del comerciante debe atender. Un atacante podría intentar inundar la web del comerciante de peticiones desde diferentes direcciones IP hasta bloquear su servicio. Para dificultarlo, el comerciante puede proponer la resolución de un problema artificial (un puzle criptográfico) a cada petición de acceso. Este pequeño problema no tendría una dificultad excesiva para un usuario real, pero resolver un gran número de pequeños problemas sería difícil para un atacante que inicia un número masivo de peticiones.

Una posible prueba de trabajo sería la siguiente: «dado un x aleatorio, encuentre el valor n (usualmente denominado «nonce» o número aleatorio de un solo uso) de forma que H(x+n) sea un *hash* que comience con cuatro ceros». Se trata de invertir una función *hash* parcialmente [hay muchos H(x+n) que comienzan con cuatro ceros]. Para hallarlo es necesario un proceso de prueba y error que consume recursos. Se puede graduar la dificultad con el número de ceros (a más ceros requeridos, mayor dificultad).

Estos conceptos básicos son suficientes para comprender el funcionamiento aproximado de Bitcoin.

Esquema C
FUNCIÓN *HASH*



FUENTE: Elaboración propia.

2.1 El objetivo de Bitcoin

Antes de comenzar a construir un esquema como Bitcoin desde cero, es necesario precisar el objetivo que se persigue. Para ello, nada mejor que recurrir al artículo de Nakamoto (2008) que dio origen al esquema. Al inicio de este se explica que el comercio a distancia por Internet depende de la intermediación de terceros, en los que los participantes en la transacción deben confiar (bancos y otros intermediarios financieros). Según Nakamoto, este modelo tiene algunas limitaciones. La primera de ellas, que no existen pagos verdaderamente irreversibles, puesto

que los intermediarios no pueden evitar el tener que mediar entre las partes en caso de disputas. El segundo problema, derivado del primero, es que los intermediarios introducen un coste, lo que hace impracticable realizar pagos casuales de pequeño importe. Lo que se necesita según Nakamoto es «un sistema de pagos electrónico basado en pruebas criptográficas en vez de en la confianza, que permita a dos actores que así lo deseen realizar una transacción entre ellos directamente sin la necesidad de un tercero de confianza». Así pues, lo que buscamos es crear un sistema de pagos electrónico similar al efectivo que permita realizar pagos a distancia sin pasar por una institución financiera. De acuerdo con el razonamiento de Nakamoto, esto permitiría implantar pagos realmente irreversibles y reduciría los costes de intermediación.

2.2 Construyendo Bitcoin

2.2.1 *TESTCOIN* VERSIÓN 0

Una vez que el objetivo está claro, una primera aproximación, muy simple, a un posible esquema de criptomoneda (llamémosla *testcoin)* podría ser el envío de un mensaje a través de Internet entre ambas partes. Si Alicia quiere pagar a Bruno, podría simplemente mandarle el siguiente mensaje: «Yo, Alicia, quiero pagar a Bruno tres *testcoin* de los veinte que me envió Cristina ayer».

Es evidente que este modelo tiene graves problemas. Incluso asumiendo que los *testcoin* que se «envían» en el mensaje tienen un cierto valor intrínseco, hay muchos detalles sin resolver: ¿cómo sabe Bruno si Alicia recibió ayer veinte *testcoin* de un tercero llamado Cristina?, ¿cómo puede estar seguro de que Alicia no ha mandado mensajes similares a otras personas y se está gastando su saldo de *testcoin* una y otra vez?, ¿cómo puede Bruno estar seguro de que el contenido del mensaje no ha sido modificado en tránsito y refleja de verdad lo que Alicia quería decir? Incluso, ¿cómo puede estar seguro de que Alicia y no otra persona le ha enviado ese mensaje?

2.2.2 *TESTCOIN* VERSIÓN 1

Aunque no es el principal problema de la versión 0 del esquema, el último problema es el más fácil de resolver. Si Alicia usa criptografía de clave pública[2], puede firmar el mensaje con su clave privada y cualquier persona podría, utilizando la clave pública de Alicia, comprobar que solo ella pudo haber escrito ese mensaje[3]. Es posible ir más allá: teniendo en cuenta que el objetivo es replicar un sistema de pagos a distancia con unas propiedades similares a las del efectivo, en realidad a Bruno no le importa que Alicia sea Alicia, solo que tenga el dinero que le entrega. Tampoco a Alicia tiene por qué importarle quién es Bruno. Por ello, se podrían asociar los saldos de *testcoin* a las claves públicas de Alicia y Bruno, que no necesitan intercambiar detalles sobre su identidad. Así, las claves públicas funcionarían como números de cuenta a los cuales podemos asociar saldos de *testcoin,* cuentas que no estarían asociadas a una identidad determinada[4].

---

2 Véase el recuadro 1 para una breve explicación no técnica sobre la criptografía asimétrica o de clave pública para asegurar la confidencialidad y autenticación de mensajes.

3 En este caso se requeriría la existencia de una entidad certificadora de confianza que verificase la identidad de Alicia cuando se generasen sus claves.

4 Al no ser necesario garantizar la identidad del participante cuando se generan las claves, no es necesario disponer de una entidad certificadora; cada usuario puede generar tantos pares de claves («cuentas») como desee usando aplicaciones estándar.

Con estas modificaciones, el mensaje que se podría enviar en la versión revisada del esquema (versión 1) podría ser similar al siguiente:

> *«Yo, clave pública 008646BBFB7D, envío 3* testcoin *que tengo asociados a dicha clave a la clave pública 3FD8C0A9C6FF»*

Alicia firmaría el mensaje con la clave privada asociada a su clave pública para que Bruno (o cualquier otro) pueda comprobar que solo la persona cuya clave pública es 008646BBFB7D pudo haber escrito ese mensaje.

La versión 1 del protocolo tiene mejor aspecto que la primera. Alicia y Bruno solo revelan sus claves públicas, y Bruno tiene la seguridad de que solo el dueño de la cuenta de origen pudo haberle enviado ese mensaje. Sin embargo, persisten los principales problemas que afectaban a la versión inicial del esquema: ¿cómo puede estar seguro Bruno de que el emisor tiene efectivamente en su cuenta los *testcoin* que envía? E, incluso, si las tuviera, ¿cómo puede estar seguro Bruno de que el emisor no está enviando un mensaje similar a varias personas gastando los mismos *testcoin* una y otra vez?

Este último problema, denominado «del doble gasto» *(double spend),* ha sido tradicionalmente el mayor obstáculo al que se enfrentaba este tipo de sistemas de pago electrónico descentralizados. Puesto que el activo que se intercambia es digital, nada impide que el emisor haga copias perfectas de él tantas veces como desee y las utilice para pagar a diferentes destinatarios. Al ser fácilmente replicable, el activo carecerá de valor. La solución habitual para evitar el doble gasto es interponer a un tercero de confianza que verifica las transacciones. Así, este intermediario recibiría el mensaje de Alicia a Bruno, verificaría que existe saldo en la cuenta de Alicia y realizaría el adeudo en su cuenta y el abono en la cuenta de Bruno. Si Alicia envía los *testcoin* a diferentes destinatarios, el intermediario rechazaría las operaciones una vez que se agote el saldo disponible. En definitiva, la solución habitual al problema del doble gasto es la introducción de un banco, justo lo que se desea evitar.

2.2.3 *TESTCOIN* VERSIÓN 2

En este punto es donde Nakamoto comenzó a desviarse de las recetas tradicionales. Puesto que un esquema en el que la información únicamente se transmite entre las dos partes que intervienen en una transacción no funciona, y puesto que se quiere evitar la existencia de un único intermediario en el que las partes deban confiar, es necesario un enfoque alternativo. La solución de Nakamoto es conservar el intermediario, pero de forma descentralizada. En otras palabras, se diseñará un esquema en el que todos los miembros del esquema conozcan todas las transacciones que han tenido lugar y las aprueben o rechacen de forma colectiva.

Así, en la versión 2 del esquema, todos los usuarios tendrán una copia completa del registro, que recoge todas las transacciones que han tenido lugar. Alicia podría enviar a Bruno un mensaje como el que se ha descrito en la versión 1 y Bruno utilizaría el historial de transacciones para comprobar que: i) efectivamente, Alicia recibió en una transacción anterior

los *testcoin* que le envía, y que ii) no los ha gastado desde entonces. Bruno añadiría la nueva transacción al registro y lo compartiría con el resto de usuarios de la red para que cada uno de ellos actualice su copia.

Sin embargo, esta versión del esquema no elimina la posibilidad de que Alicia intente realizar un doble gasto. Alicia podría enviar casi simultáneamente dos mensajes similares transfiriendo los mismos *testcoin* a Bruno y a Cristina. Bruno y Cristina comprobarían que ambas transacciones son posibles de acuerdo con sus copias del registro, las añadirían a este y compartirían sus versiones del registro (divergentes) con el resto de los usuarios. Esta incoherencia haría prácticamente imposible mantener una versión unificada del registro entre los participantes del esquema.

2.2.4 *TESTCOIN* VERSIÓN 3

Para resolver este problema, se puede pasar a una versión 3 del protocolo, introduciendo un cambio en el método de verificación. En vez de dejar que Bruno o Cristina verifiquen las transacciones individualmente y propaguen versiones potencialmente divergentes del registro, se exigirá que la verificación sea conjunta por parte de todos los usuarios. Así, cuando Alicia envíe el mensaje a Bruno, este no lo comprobará en solitario, sino que lo publicará en la red para que todos los usuarios sepan que Alicia (en realidad, solo conocen su clave pública) quiere enviar unos *testcoin* a Bruno (del que solo conocerán también su clave pública). Bruno invitará a todos los usuarios a decidir si la operación es correcta y, por tanto, si debe registrarse o no. Si Alicia trata de pagar de forma casi simultánea a Bruno y a Cristina, los usuarios de la red se darán cuenta de que ambas operaciones son incompatibles y elegirán cuál debe registrarse y cuál se debe rechazar, asegurando en todo momento que el registro se mantiene único.

A primera vista, esta modificación parece prometedora, pero deja algunos cabos sueltos. El principal es el acuerdo entre los participantes: ¿cómo es posible asegurar que los participantes en el esquema están de acuerdo sobre qué operaciones pueden incorporarse al registro y cuáles no? Quizás la forma más sencilla de resolver el problema es por votación, otorgando un voto a cada uno de los participantes en la red, de forma que aquellas transacciones que sean votadas por una mayoría sean incorporadas al registro compartido. Este enfoque tiene un problema fundamental, y es que es relativamente fácil construir un gran número de identidades falsas y tratar de engañar a la red. Alicia podría (con un coste muy moderado) inundar la red de identidades ficticias que votasen a favor de incluir en el registro el pago tanto a Bruno como a Cristina, engañando a ambos y dando por bueno un registro incoherente.

2.2.5 *TESTCOIN* VERSIÓN 4

Para resolver el problema del acuerdo entre los actores de la red, se ha de pasar a la versión 4 del esquema, en la que se introduce la principal innovación de Nakamoto y probablemente la menos intuitiva. Para evitar que un actor deshonesto engañe al sistema con un gran número de identidades falsas, se requerirá que el proceso de aprobación de transacciones sea artificialmente difícil, realizando lo que se denomina una «prueba de trabajo» *(proof of work).* De esta forma, el historial de transacciones aceptado por los participantes en el esquema no

será el que más votos reúna (los votos son fáciles de falsificar), sino el que mayor trabajo computacional incorpore. Lógicamente, es necesario dar un incentivo a los participantes para que lleven a cabo ese trabajo, que consume recursos en forma de electricidad e inversión en *hardware.* Por ello, la verificación se verá recompensada con una asignación de *testcoins* recién acuñados. A continuación se describe este procedimiento con algo más de detalle.

Cuando Alicia desea enviar su pago a Bruno, el mensaje se publica para todos los participantes, junto con otras transacciones candidatas a incorporarse al registro. Los participantes tienen acceso al historial de transacciones, por lo que pueden verificar sin apenas coste computacional si ese conjunto de nuevas operaciones (que se denominará un «bloque» de transacciones) es coherente con el historial del registro. Es decir, se comprueba que los emisores recibieron fondos anteriormente y no los han gastado, así como que las operaciones que se están verificando dentro del bloque son compatibles entre sí y no producen doble gasto. En caso de que así sea, ese bloque de transacciones podría añadirse al registro.

Antes de incorporarlo, sin embargo, se exige que se realice una prueba de trabajo. En concreto, se requiere que algún usuario encuentre un valor x *(nonce)* de forma que el resultado de obtener el *hash*[5] de la información del bloque (básicamente, el listado de transacciones que se desea incorporar al registro más una información de cabecera), junto con el *nonce,* dé como resultado un valor que comience con un número determinado de ceros.

H(información del bloque, *nonce)* = valor que comience con n ceros

donde:

Información del bloque = cabecera + listado de transacciones

Según se explica en el esquema 1, el resultado de la función *hash* no es predecible, por lo que encontrar el nonce implica un trabajo computacional que solo puede resolverse mediante fuerza bruta: se trata de probar diferentes valores de x al azar, hasta que se encuentre uno que cumpla con la condición requerida. El número n de ceros requerido al inicio se puede ajustar para que el trabajo tenga mayor o menor dificultad para los usuarios que quieran actuar como verificadores de transacciones.

De esta forma, los verificadores, llamados «mineros», compiten por ser los primeros en encontrar una solución a este problema artificial. Cuando un minero encuentra una solución, la publica para que todos los usuarios comprueben que es correcta, un proceso muy sencillo[6]. Una vez comprobadas la validez de las transacciones (existencia de saldo y ausencia de doble gasto) y la validez de la solución de la prueba de trabajo, los mineros incorporan el bloque al registro y continúan trabajando en la generación de nuevos bloques.

---

5 Para una descripción básica de la función *hash,* se puede consultar el recuadro 1.

6 Es muy difícil obtener un *nonce* x para que h(información del bloque, x) tenga unas propiedades determinadas (p. e., que comience con n ceros). Sin embargo, si se conoce x, es muy sencillo desde un punto de vista computacional hallar h(información del bloque, x) y verificar que la solución cumple con la condición requerida.

Queda por resolver un aspecto importante, como es el orden de las operaciones. El registro que estamos construyendo es esencialmente un listado de transacciones ordenado cronológicamente al que se le van añadiendo bloques de operaciones paulatinamente. El orden cronológico de los bloques es esencial para saber si una operación se puede realizar o no. Por ello, cada nuevo bloque que se incorpora al registro incluye una referencia que apunta al bloque inmediatamente anterior. Esta referencia se puede obtener con facilidad insertando en la cabecera de cada bloque el *hash* del bloque anterior. Con esto creamos una cadena de bloques o *blockchain*[7].

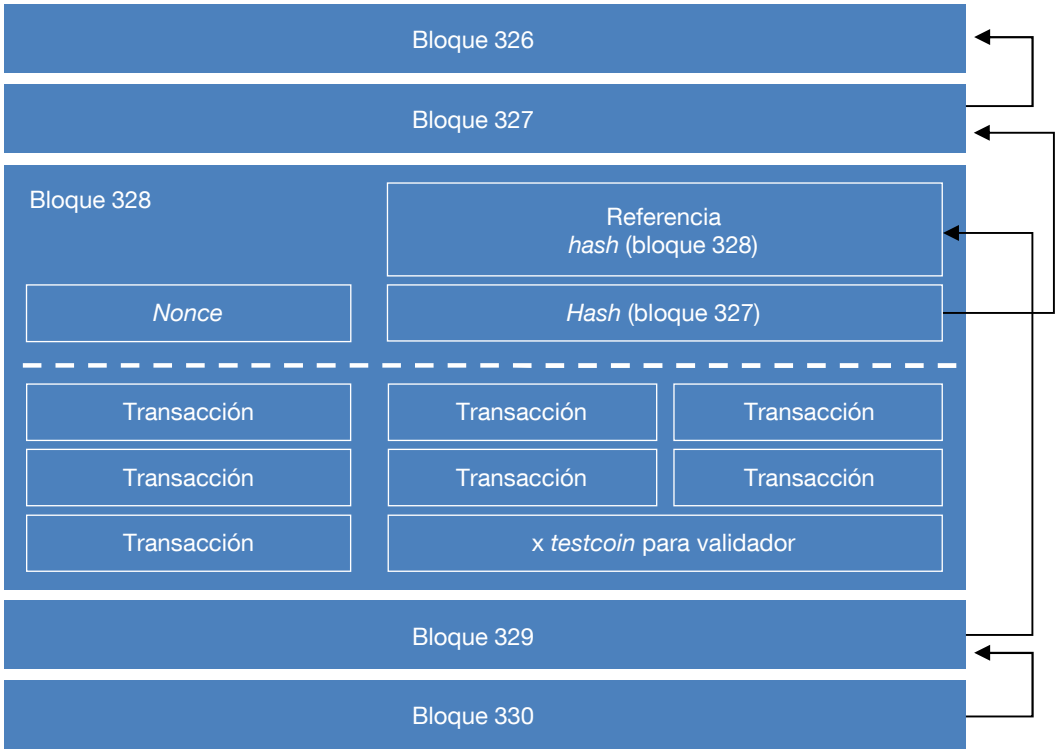
Finalmente, hay que dar un incentivo a los mineros para que gasten su tiempo y dinero (compra de *hardware* y gasto en electricidad) en buscar soluciones a la prueba de trabajo. Para ello, cada minero añade a las transacciones del bloque sobre el que está realizando la prueba de trabajo un pago adicional en el que el propio minero se asigna una cantidad determinada de *testcoins.* Estos *testcoins* no provienen de ninguna transacción previa, sino que se crean como recompensa por el trabajo realizado para obtener el *nonce* requerido.

Esto es todo lo necesario. Con algunas simplificaciones, la versión 4 de *Testcoin* refleja el funcionamiento básico del protocolo de *Bitcoin.* El esquema 2 resume los aspectos básicos del *blockchain* que acabamos de crear.

7 El primer bloque de la cadena o bloque génesis de Bitcoin contenía simplemente un titular de la portada del *Times* del 3 de enero de 2009 («The Times 03/Jan/2009 Chancellor on brink of second bailout for banks»), junto con una asignación de 50 *bitcoins* para el minero que generó el bloque (presumiblemente, el propio Nakamoto).

ESQUEMA DEL *BLOCKCHAIN* DE TESTCOIN

ESQUEMA 2



FUENTE: Elaboración propia.

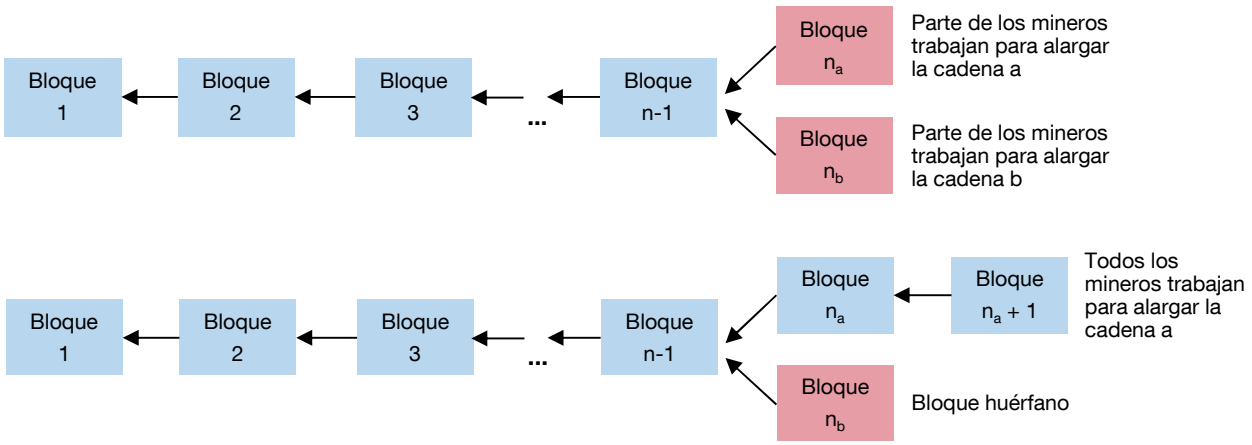
El esquema que se ha descrito, desde un punto de vista práctico, se recoge en un *software* de uso público que cualquier persona puede descargar de Internet y hacer funcionar en su ordenador para realizar operaciones o para tratar de verificarlas como minero. Tampoco existe limitación de entrada o salida de la red, que es completamente libre. Teniendo en cuenta la complejidad actual de la prueba de trabajo, sin embargo, los mineros suelen ser entidades profesionales especializadas y con un equipo diseñado al efecto. Tampoco los usuarios participan normalmente en Bitcoin de forma directa, sino que suelen adquirir sus *bitcoins* en casas de cambio (que venden criptoactivos por dinero de curso legal o intermedian en la compraventa a cambio de una comisión) y custodian las claves de sus *bitcoins* en aplicaciones monedero *(wallet)* o en entidades especializadas.

2.3 ¿Cómo se mantiene el registro único? Las bifurcaciones de la cadena

Quizás la primera pregunta que surge, una vez explicado el funcionamiento básico de Bitcoin, es la de si una multitud de verificadores desconocidos y repartidos por todo el mundo, entre los que no hay ninguna relación de confianza, son capaces de mantener un registro de transacciones unificado. En realidad, el registro puede tener ramas o estar bifurcado de forma transitoria, como se explica a continuación.

El protocolo de Bitcoin determina que la cadena lineal más larga (que es aquella que incluye más bloques y, por tanto, la que incorpora una mayor prueba de trabajo computacional) constituye la versión correcta del registro de transacciones. Por otro lado, Bitcoin es una red global con multitud de nodos, por lo que el intercambio de información entre nodos no es instantáneo. Podría darse el caso de que dos validadores, casi al mismo tiempo, encuentren dos soluciones válidas para el último bloque de la cadena. Cada validador anunciará al resto de nodos su solución y, considerando la latencia de la red, es probable que las dos soluciones se propaguen de forma desigual, de manera que algunos nodos aceptarán la solución n_a y otros la n_b.

BIFURCACIONES EN EL *BLOCKCHAIN* ESQUEMA 3



FUENTE: Elaboración propia.

El registro se habrá bifurcado en dos cadenas de igual longitud, por lo que algunos mineros trabajarán para alargar una de las cadenas y otros para alargar la otra. Podría ocurrir que se repita la coincidencia de que se encuentren soluciones casi simultáneamente, pero, en un espacio breve de tiempo, algún grupo de mineros generará un bloque para una de las dos ramas y será capaz de comunicar esa solución a toda la red antes de que se encuentre solución para la otra. Supongamos que se genera antes el bloque n_a+1; en ese caso, todos los verificadores, independientemente de la rama en la que estuvieran trabajando, verán que la cadena que más trabajo incorpora es la que tiene n+1 bloques. Todos se trasladarán al último bloque de esa cadena y trabajarán para alargarla, generando el bloque n_a+2. Con esto se recuperan de forma automática el consenso y la unicidad del registro.

El bloque n_b se denomina «bloque huérfano» y las transacciones incluidas en ese bloque que no estén ya incorporadas a la cadena[8] vuelven a considerarse transacciones pendientes de verificación.

2.4 ¿Cuándo podemos decir que una transacción es definitiva?

Una consecuencia del funcionamiento descrito en el apartado anterior es la dificultad para determinar de forma precisa cuándo se puede dar por ejecutada una operación en Bitcoin. Volviendo al esquema 3 que se analizaba en el apartado anterior, imaginemos una transacción que esté incluida en el bloque n_b pero que no esté incluida en el n_a ni en el n_a+1. El beneficiario creería que su operación se ha incorporado al *blockchain,* cuando en realidad solo se ha incorporado a una rama que ha dejado de estar en el tronco principal de transacciones. Una vez que se confirma que el bloque n_b es un bloque huérfano, la transacción vuelve a quedar pendiente de confirmación. Por ello, se recomienda que los receptores esperen a que se añadan varios bloques (al menos, cinco) para asegurarse de que la transacción se ha incorporado al tronco principal del *blockchain.* Así, la irrevocabilidad de la operación no se obtiene en un momento concreto, sino que es un proceso gradual en el que la certeza de que aquella se ha producido no es absoluta ni está garantizada, sino que aumenta a medida que se añaden bloques a la cadena.

2.5 ¿Cómo se protege Bitcoin ante intentos de fraude?

Es necesario resaltar que el sistema, por construcción, permite evitar los fraudes más directos. Por ejemplo, todas las transacciones deben ir firmadas con la clave privada asociada a la cuenta del emisor, por lo que no es posible que un verificador introduzca un pago fraudulento y se apropie directamente de un saldo propiedad de otra persona transfiriéndolo a una cuenta bajo su control.

Tampoco es posible que un verificador incluya en un bloque una transacción irregular (enviando un saldo mayor que el disponible) o dos operaciones incompatibles entre sí (por ejemplo, derivadas de enviar el mismo saldo a dos personas diferentes). Aunque el verificador

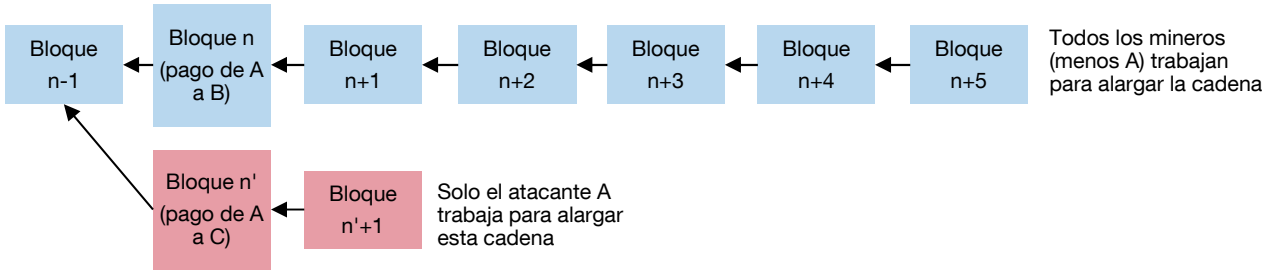
8 Cuando se generaron los bloques n_a y n_b, los validadores que generaron dichos bloques eligieron las transacciones que incorporaron al bloque del conjunto de transacciones pendientes. Es posible, por tanto, que algunas (o todas, o ninguna) de las transacciones que se incluyeron en el bloque n_a estén también incluidas en el bloque n_b.

en cuestión consiguiera encontrar un *nonce* válido para generar el bloque, ningún otro nodo lo reconocería como correcto a la vista del historial de transacciones, que es público.

Sin embargo, otros tipos de fraude sí son posibles, aunque el diseño del sistema hace que su probabilidad de éxito sea prácticamente despreciable. En concreto, se podría considerar la posibilidad de tratar de engañar al sistema sin vulnerar ninguna regla. Imaginemos que Alicia envía 10 *bitcoins* a Bruno, que la transacción se incorpora a un bloque n y se añaden cinco bloques adicionales a la cadena. Cuando la cadena alcanza la longitud n+5, conforme a la regla descrita en el apartado anterior, Bruno se declara satisfecho y confirma que ha recibido el pago. En ese momento, Alicia podría elaborar un bloque n alternativo (llamémoslo «n'») en el que retira su pago a Bruno y lo sustituye por un pago a otra clave pública controlada por la propia Alicia. Si fuese capaz de convencer al resto de participantes de que el nodo n' es correcto y no el n, habría conseguido defraudar a Bruno. En otras palabras, Alicia podría intentar alterar el historial para deshacer un pago realizado por ella misma anteriormente y recuperar los fondos.

Para lograr eso, Alicia se enfrenta a una serie de dificultades. La primera es realizar la prueba de trabajo para encontrar un *nonce* para el bloque n', puesto que al cambiar una transacción cambia la información del bloque, con lo que el *nonce* previo deja de ser válido. Si Alicia encontrase la solución, no podría convencer al resto de mineros de que su cadena (con n bloques, incluyendo el último falsificado) es la correcta, puesto que existe una cadena más larga con n+5 bloques. Esta última incorpora más pruebas de trabajo, por lo que el resto de mineros la acepta como correcta. Alicia podría entonces tratar de encajar el bloque n' en la cadena correcta de n+5 bloques, pero esto no es posible, puesto que el puntero del bloque n+1 apunta al bloque n, no al n' (es el *hash* del bloque n, no el del n'). Alicia tendría que cambiar el puntero en el bloque n+1 por el *hash* de n', pero al cambiar la información del bloque n+1 [(que pasa a ser el (n+1)'] el *nonce* de dicho bloque dejaría de ser válido, por lo que deberá realizar la prueba de trabajo del bloque (n+1)', y así sucesivamente. En definitiva, Alicia tendría que rehacer la cadena de bloques por su cuenta (ningún minero querrá gastar recursos en minar bloques de una cadena tan corta) y conseguir que supere la longitud de la cadena correcta para que pueda ser aceptada por el resto de participantes; mientras tanto, el resto de mineros preferirá alargar la cadena correcta y tratar de obtener las recompensas correspondientes. Si Alicia no tiene más poder de computación que el resto de mineros juntos, es prácticamente seguro que el ataque fracasará. Alicia no solo no conseguirá acercarse a la longitud de la cadena verdadera, sino que perderá terreno progresivamente y nadie reconocerá el historial de transacciones que propone. Estará consumiendo recursos en balde.

En vez de proteger al sistema de intentos de fraude con medidas de seguridad al uso, Bitcoin opta por permitir este tipo de conductas (no vulneran ninguna regla del sistema), pero las desincentiva por construcción. Si Alicia tiene menos poder de computación que el resto de mineros de forma agregada, es más rentable para ella cooperar con el sistema, generando bloques y obteniendo las recompensas, que enfrentarse a él. Si Alicia tiene más poder de computación que el resto de nodos, el sistema será en realidad un sistema centralizado y dejará de ser atractivo para los usuarios.



FUENTE: Elaboración própia.

2.6 ¿Dónde se almacenan los saldos de bitcoins?

El *blockchain* de Bitcoin es esencialmente un listado cronológico de transacciones, por lo que cabe preguntarse dónde se registran los saldos disponibles para cada usuario. Para entender el proceso que permite a los usuarios enviar y recibir *bitcoins* y calcular los saldos disponibles es necesario tener un conocimiento básico de las transacciones registradas en el *blockchain.*

Las transacciones son de dos tipos: las más habituales son aquellas que tienen varios *inputs* (saldos recibidos en transacciones anteriores) y varios *outputs* (saldos enviados a otros destinatarios). El segundo tipo es la recompensa a los mineros, que no tiene inputs pero sí un *output* en forma de *bitcoins.* Esta configuración permite a los usuarios enviar cantidades exactas, pagar comisiones, agregar saldos y recibir la vuelta de un pago, como se verá a continuación.

Supongamos que Alicia es una usuaria de la red y recibió, en la transacción t_1, un saldo de 5 *bitcoins,* en la transacción t_2 un saldo de 3 *bitcoins* y en la transacción t_3 un saldo de 1 *bitcoin.* Estos saldos fueron *outputs* de dichas transacciones y están asociados a tres cuentas (claves públicas) cuya contraseña (clave privada asociada) solo conoce Alicia. Hasta el momento, Alicia no ha realizado ningún pago, pero ahora desea pagar a Bruno 2 *bitcoins* y a Cristina 4 *bitcoins.* Además, para incentivar el proceso de la operación, desea incluir una comisión de 0,1 *bitcoins* para el minero que incluya la transacción en un bloque.

Para realizar estas operaciones, Alicia construye una transacción t_4 en la que se recogen como *inputs* las cantidades recibidas en las transacciones t_1 y t_2 (5 y 3 *bitcoins)* y como *outputs* los pagos a Bruno (2) a Cristina (4) y la «vuelta» del pago (1,9), que Alicia envía a una nueva dirección pública controlada por ella misma. El resto (0,1) es la comisión al minero que incorpore la transacción en el *blockchain.* Cristina firma la transacción con las claves privadas asociadas a las cuentas de origen (t_1 y t_2) y dirige los *outputs* a las claves públicas de los destinatarios.

Si Alicia quisiera averiguar su saldo, tendría que agregar los fondos que ha recibido como *output* en algún momento y que no haya utilizado como *input* de una transacción posteriormente. Después de realizar la transacción t_4, el saldo final de Alicia (2,9) se calcula agregando los saldos recibidos en t_3 (1) y t_4 (1,9). En resumen, en el *blockchain* de Bitcoin los saldos no se registran, sino que se construyen indirectamente agregando los saldos recibidos pero no gastados de las direcciones (cuentas) propiedad de un usuario determinado. Este procedimiento se denomina «UTXO» (*unspent transaction output).*

2.7 Algunas cifras[9]

En la actualidad, el esquema Bitcoin tiene un tamaño muy reducido desde el punto de vista cuantitativo. Como ya se ha señalado, la creación de *bitcoins* está asociada a la generación de bloques, de forma que los nuevos *bitcoins* se otorgan al verificador que encuentra la solución a la prueba de trabajo. Esta recompensa fue inicialmente de 50 *bitcoins* por bloque, pero el protocolo establece que se reduzca a la mitad cada 210.000 bloques. Teniendo en cuenta que se crea un bloque cada 10 minutos aproximadamente[10], esta regla establece un ritmo de creación decreciente, con las recompensas reduciéndose a la mitad cada cuatro años. En la actualidad, la recompensa es de 12,5 *bitcoins* por bloque y se han emitido ya unos 17,5 millones de *bitcoins.* Si la regla de creación no se modifica en versiones futuras del protocolo, se estima que se emitirán un total de 21 millones de unidades, en un proceso que se alargará hasta el año 2140.

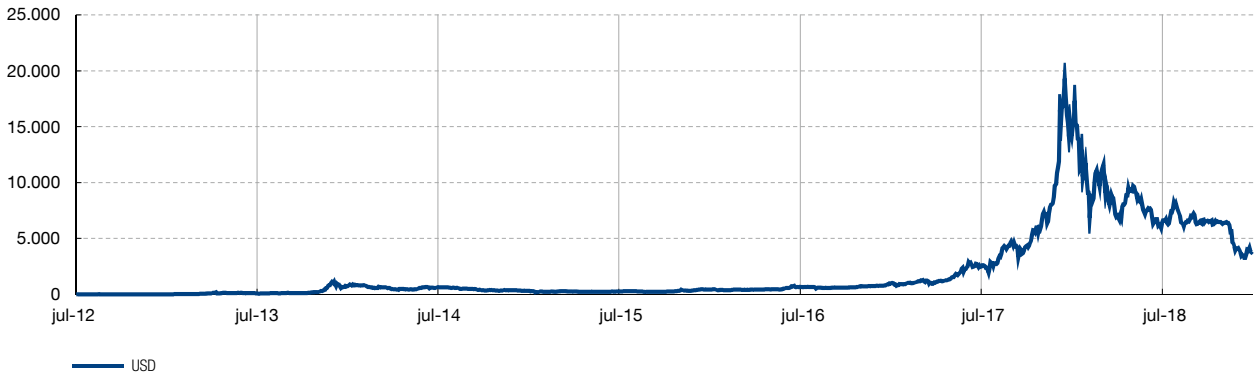
La cotización del *bitcoin* es muy volátil. Tras el tremendo incremento que experimentó en la última parte de 2017 (hasta casi rozar los 20.000 USD por *bitcoin),* su precio ha descendido notablemente entre fuertes oscilaciones (véase gráfico 1). A finales de 2018, su precio se sitúa en torno a 3.500 USD por *bitcoin* por lo que el valor total aproximado de los *bitcoins* emitidos se encuentra cercano a los 60.000 millones USD.

9 Cifras obtenidas de www.blockchain.com (diciembre de 2018).

10 La tasa de creación de bloques se mantiene en media constante, ya que el protocolo Bitcoin ajusta automáticamente la dificultad de la prueba de trabajo para que se genere un bloque cada 10 minutos en media, independientemente del poder de computación de los verificadores.

COTIZACIÓN DEL *BITCOIN* EN USD

GRÁFICO 1



FUENTE: https://www.blockchain.com.

El sistema procesa unas 250.000 transacciones diarias por un total estimado de 150.000 *bitcoins*[11] (unos 600 millones de USD). Estas cifras son insignificantes si las comparamos con los sistemas de pago tradicionales. Como comparación, según la *Memoria anual sobre la vigilancia de las infraestructuras de los mercados financieros* (Banco de España, 2018), el principal sistema de pagos minorista español (Sistema Nacional de Compensación Electrónica, SNCE) procesó en media diaria durante 2017 unos 7,2 millones de pagos, por unos 7.000 millones de euros. Hay que considerar que el SNCE presta servicio fundamentalmente a las personas físicas y a empresas no financieras en un país de 46 millones de habitantes, mientras que Bitcoin es un esquema global.

11 Estimaciones construidas deduciendo las cantidades de cambio devueltas a los emisores. Esta estimación incluye tanto operaciones de compraventa de *bitcoins* con moneda fiduciaria como operaciones de compra de bienes o servicios, así como otras transacciones sin significado económico claro (p. e., traspaso de saldos entre direcciones controladas por un mismo usuario).

3 ¿Es Bitcoin un buen sistema de pago?

Dejando de lado los aspectos estrictamente monetarios del *bitcoin* (su uso como unidad de cuenta, medio de cambio o depósito de valor), este apartado se centra en el funcionamiento del *blockchain* de Bitcoin como mecanismo de intercambio alternativo a los sistemas de pago tradicionales. Teniendo en cuenta que Bitcoin fue creado para el comercio electrónico y la realización de pagos casuales en Internet [Nakamoto (2008)], parece razonable centrar el análisis en las operaciones de pago minoristas.

Los criterios utilizados para evaluar Bitcoin como un sistema de pago minorista serán los siguientes: seguridad, rapidez, coste, privacidad, escalabilidad, eficiencia y sostenibilidad del modelo de negocio a lo largo del tiempo.

3.1 Seguridad

Los defensores de Bitcoin presentan su seguridad como uno de los puntos fuertes del esquema. El historial de transacciones es muy fiable, debido al encadenamiento de bloques mediante técnicas criptográficas y resulta prácticamente imposible alterar este historial, a menos que una mayoría de validadores colusionen para falsificar el *blockchain.* Por otro lado, la seguridad de los saldos registrados en el *blockchain* se garantiza mediante un sistema de claves públicas y privadas. En aparente contradicción con este elevado nivel de seguridad, son frecuentes las noticias sobre robos de *bitcoins.*

Para analizar este aspecto, es necesario separar entre la seguridad del núcleo del esquema (el *blockchain* de Bitcoin) y la seguridad del esquema en su conjunto, incluyendo las aplicaciones monedero o las casas de cambio.

La columna vertebral de Bitcoin es el *blockchain,* el registro público que contiene el historial completo de transacciones. Teniendo en cuenta que los saldos de los usuarios se determinan de forma indirecta a través de las cantidades recibidas y no gastadas aún, todo el esquema se basa en la confianza de que el historial de estas transacciones es único y no permite alteraciones. El encadenamiento criptográfico de los bloques hace que cualquier alteración del *blockchain* sea inmediatamente detectable.

¿Significa esto que es seguro utilizar Bitcoin? No necesariamente, desde el punto de vista del usuario final. Incluso si el registro compartido es resistente a la falsificación y el núcleo del sistema funciona con seguridad, los usuarios pueden sufrir robos (y, de hecho, los sufren con frecuencia)[12]. Los usuarios no están identificados y el sistema es descentralizado, por lo que la propiedad de los *bitcoins* se demuestra con la posesión de la clave privada asociada a la dirección en la que esos *bitcoins* están almacenados en el *blockchain.* Si el usuario pierde

12 Según algunas estimaciones, un 14 % del total de *bitcoins* y de otras criptomonedas emitidas podría haber sido robado a sus propietarios (https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies).

la clave privada asociada a una dirección, de hecho pierde los *bitcoins* (seguirían registrados en el *blockchain,* pero el usuario no podría utilizarlos, haciéndolos inservibles). Si un atacante roba la clave privada, podrá realizar una transacción enviando los *bitcoins* de otro usuario a otra cuenta bajo su control. Como la clave privada identifica al dueño de los *bitcoins,* la transacción correspondiente al robo sería indistinguible de cualquier otra transacción y es compatible con un funcionamiento correcto del *blockchain.*

En principio, los usuarios pueden operar de forma directa en el esquema, sin intermediarios, por lo que el propio usuario podría custodiar sus claves privadas. Sin embargo, esto requiere conocimientos informáticos que no están al alcance de todos los usuarios. Para operar en el esquema, la mayor parte de los usuarios finales confía en proveedores de monederos digitales y casas de cambio que custodian las claves de sus clientes como parte de sus servicios. Los incidentes de seguridad más notorios en relación con Bitcoin han tenido lugar en este tipo de entidades que se sitúan en la periferia del esquema y hacen las veces de interfaz entre la red Bitcoin y los usuarios finales. Estas entidades no suelen estar reguladas o supervisadas, y es frecuente que los usuarios no tengan a quién acudir ante un robo en sus cuentas o ante la quiebra de la entidad que custodia los saldos. Uno de los casos más notorios tuvo lugar en febrero de 2014, cuando una de las principales empresas para el intercambio de *bitcoins* por dinero de curso legal, Mt Gox, quebró en circunstancias poco claras, dejando a muchos usuarios sin sus fondos.

En contraposición, las cuentas bancarias y las operaciones de pago a través de sistemas tradicionales son ofrecidas por entidades supervisadas que cuentan con amplia experiencia en la seguridad de la información. Además, en caso de fraude, la regulación protege a los usuarios, que pueden reclamar a las entidades financieras el reintegro de los fondos perdidos a partir de ciertas cantidades.

3.2 Rapidez

A menudo se menciona la rapidez como una de las cualidades fundamentales de Bitcoin, en comparación con los pagos tradicionales a través de intermediarios financieros, ya que Bitcoin supuestamente permite realizar una operación de principio a fin en 10 minutos por término medio. Sin embargo, esta rapidez no se logra siempre y necesita ser matizada, por varias razones.

En primer lugar, la rapidez del proceso depende de la comisión incluida en la operación: una transacción que no incluya comisiones o con comisiones muy bajas puede permanecer largo tiempo en cola de espera o no procesarse nunca. En segundo lugar, una vez incorporada la transacción al *blockchain* de Bitcoin, se recomienda al receptor esperar a que se añadan cinco bloques a la cadena para tener una cierta seguridad de que los fondos se hallan realmente en su poder. Esta espera adicional (de unos 50 minutos por término medio) se recomienda para descartar la posibilidad de que el bloque en el que se ha integrado la operación resulte ser finalmente un bloque huérfano en una rama del *blockchain* que no acabe formando parte del historial de transacciones.

En definitiva, la rapidez de Bitcoin no es tan elevada como a veces se indica y, además, la velocidad de proceso es poco predecible de antemano. Aunque la rapidez de Bitcoin puede resultar una ventaja comparativa en ciertos segmentos del mercado de pagos, como los pagos internacionales por corresponsalía bancaria, no es llamativa en comparación con los pagos realizados en un entorno nacional. En la actualidad, es posible hacer pagos con mayor rapidez utilizando una arquitectura centralizada e intermediarios financieros tradicionales. Por ejemplo, los pagos con tarjeta ofrecen al usuario una experiencia de pago casi inmediata, y existe la posibilidad de realizar transferencias inmediatas entre cuentas bancarias en cuestión de segundos mediante la utilización del móvil o de la banca por Internet.

3.3 Coste

Inicialmente, los defensores de Bitcoin argüían que la red permitía transacciones gratuitas, aunque se podía incluir una pequeña cantidad de manera voluntaria en concepto de comisión. Estas comisiones suponían una donación al minero que lograse incluir la transacción en un bloque y constituían, por tanto, un pequeño incentivo para que el minero en cuestión diese prioridad al proceso de esa operación (los mineros pueden escoger las transacciones que incorporan a un bloque, por lo que elegirán las transacciones que incluyan las mayores comisiones).

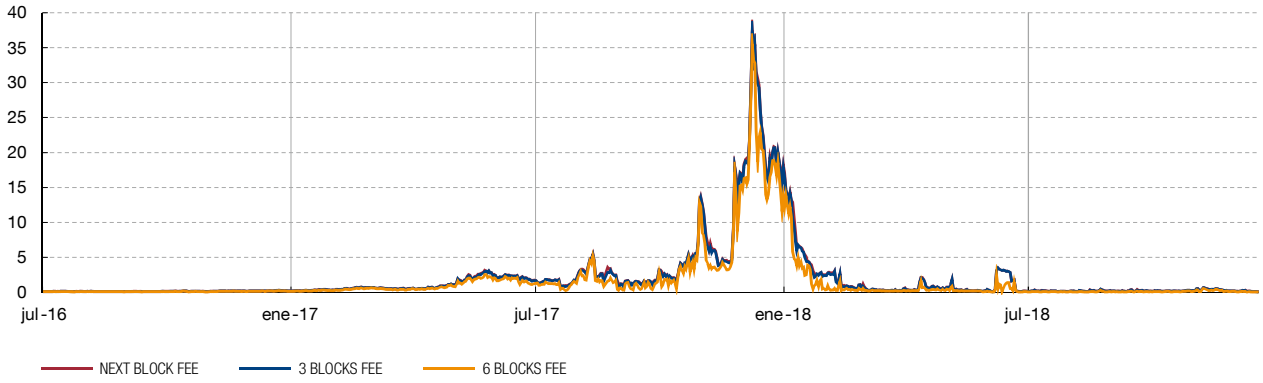
En la actualidad, sin embargo, las transacciones de *bitcoins* están sujetas a comisiones de forma generalizada. Con el paulatino incremento del tráfico en la red, ha aumentado significativamente el número de transacciones candidatas a integrarse en un bloque para ser procesadas. Teniendo en cuenta que el tamaño de un bloque está limitado (actualmente, a 1 MB) y que la tasa de producción de bloques permanece constante en términos medios (aproximadamente, un bloque cada 10 minutos), en la actualidad solo se procesan en un tiempo razonable las transacciones que incluyen comisiones. Las transacciones sin comisión permanecen indefinidamente en cola mientras continúe entrando en la red un número suficiente de operaciones con comisiones para los mineros. La comisión mínima que asegura la tramitación en un lapso de tiempo reducido varía en función del tráfico de la red y, lógicamente, tiende a aumentar con el incremento de tráfico.

Algunos monederos digitales de *bitcoin* incluyen por defecto comisiones fijas por operación (aunque su nivel es parametrizable por el usuario), mientras que otros monederos, más modernos, establecen una comisión de forma dinámica en función del tráfico en la red.

Las comisiones dependen fundamentalmente de la extensión de la operación y no del importe transmitido, por lo que tienden a ser relativamente bajas para pagos de alto importe y relativamente altas para micropagos (precisamente, el caso de uso que se menciona en el informe original que dio pie a la creación del sistema). Por dar una idea del orden de magnitud, las comisiones mínimas que aseguran un procesamiento casi inmediato de una transacción de tamaño habitual suponen unos 20 céntimos de dólar (diciembre de 2018), pero llegaron a superar los 35 USD en diciembre de 2017 (coincidiendo con una tremenda apreciación del *bitcoin* y con un incremento del número de transacciones en la red).

COMISIÓN DE TRANSACCIONES, EN USD

GRÁFICO 2



FUENTE: https://bitcoinfees.info/.

Teniendo en cuenta la disminución paulatina de las recompensas a los mineros y el límite de memoria establecido por bloque, es previsible que cualquier aumento significativo de tráfico en la red cause subidas repentinas de las comisiones, a menos que se introduzcan cambios sustanciales en el diseño del sistema.

Por otro lado, y a menos que el usuario desee mantener un saldo en *bitcoins* de manera indefinida, a las comisiones directamente relacionadas con el procesamiento de transacciones hay que añadirles el coste de conversión al cambiar los *bitcoins* por moneda fiat. Este coste, que rara vez se menciona, puede ser sustancial.

3.4 Anonimato y privacidad

El esquema Bitcoin se presenta como un sistema de pagos anónimo, a pesar de estar basado en un registro público. En los sistemas de pago tradicionales, normalmente la información personal de los participantes en la operación (nombres, números de cuentas, concepto del pago) se transmite con el mensaje de la operación. Esta información es accesible en todo o en parte para el emisor, receptor e intermediarios, pero no para terceros no autorizados. Bitcoin cambia radicalmente este enfoque, ya que toda la información sobre las transacciones es pública (básicamente, números de cuenta e importes), pero no se incluyen datos que puedan relacionar a emisor o receptor con una cuenta determinada. El anonimato es, pues, compatible con el carácter público del *blockchain* y se presenta como una ventaja de Bitcoin, ya que se puede utilizar el sistema sin proporcionar información personal que pueda ser robada.

Aunque el deseo de anonimato puede tener razones legítimas[13], esta característica de Bitcoin ha sido muy criticada por diversas autoridades, especialmente si se tiene en

13 Pensemos, por ejemplo, en una transacción por Internet entre un usuario y un comerciante con el que nunca ha operado y en el que no tiene confianza. El usuario podría preferir pagar de forma anónima para evitar que el comerciante acceda a detalles personales (nombre, número de tarjeta, fecha de caducidad) que puedan ser utilizados de manera fraudulenta posteriormente si el comerciante no custodia la información correctamente.

cuenta que es una red de alcance mundial en la que operan múltiples intermediarios que no pertenecen al ámbito financiero. El anonimato dificulta la aplicación de medidas para prevenir el blanqueo de dinero y la financiación del terrorismo, y facilita por tanto la utilización del sistema para transacciones relacionadas con actividades ilícitas. Quizás el caso más notorio sea el de *Silk Road,* un portal de venta de sustancias y servicios ilegales alojado en la Internet profunda, cuyo medio de pago era, precisamente, el *bitcoin.* En octubre de 2013, el FBI desmanteló este portal, incautándose en la operación 26.000 *bitcoins*[14].

Sin embargo, el presunto anonimato de Bitcoin es mucho menor de lo que podría pensarse en un principio. Aunque es cierto que el *blockchain* no contiene información personal, la mayoría de los usuarios normalmente se identifican ante algún intermediario[15] (una casa de cambio, por ejemplo) la primera vez que acceden a la red y cambian moneda real por *bitcoins* (y, posteriormente, al vender *bitcoins* a cambio de otras monedas). Una vez que se dispone de *bitcoins,* el usuario puede utilizar un número ilimitado de cuentas diferentes y dividir o combinar sus saldos. Aunque las transferencias entre las cuentas de un mismo usuario son, en principio, indistinguibles de las operaciones entre diferentes usuarios, el carácter público del registro hace que sea posible un análisis estadístico detallado de las transacciones. Este análisis, en combinación con otras fuentes de información (por ejemplo, la identificación de un usuario al cambiar moneda o el vínculo entre una cuenta y una identidad en un blog), permite en muchos casos identificar las cuentas de un mismo usuario y relacionarlas con una identidad concreta[16].

3.5 Capacidad

La configuración actual de Bitcoin impone un límite al número de pagos que puede procesar el esquema. Si tenemos en cuenta que la tasa de producción de bloques se mantiene constante (por término medio, 10 minutos), que cada bloque tiene un tamaño máximo de 1MB y que un pago típico en la red supone unos 250 *bytes*[17], un bloque podría contener algo más de 4.000 transacciones, lo que supone unas 7 transacciones por segundo (o unas 600.000 operaciones diarias). Aunque estas cifras son significativas, son órdenes de magnitud inferior a las habituales en los sistemas minoristas actuales, especialmente teniendo en cuenta que Bitcoin es una red global. Como referencia, los esquemas internacionales de pago con tarjetas son capaces de procesar miles de operaciones por segundo.

El uso efectivo de la red ha estado bastante cercano a la capacidad máxima a principios de 2018, momento en el que las comisiones por operación se dispararon, coincidiendo con el incremento de transacciones y la subida de la cotización.

---

14 Por un valor en aquel momento de 3,5 millones de dólares. Se estimó que en los 2,5 años de operación del portal se pudieron haber llevado a cabo transacciones por 1.200 millones de dólares [véase Halaburda *et al.,* (2016)].

15 En la UE, por ejemplo, las casas de cambio de criptoactivos son sujetos obligados a reportar a las autoridades, a fin de combatir el lavado de dinero y la financiación del terrorirsmo.

16 Existen también técnicas y servicios para «oscurecer» el rastro de fondos y tratar de aumentar el anonimato en la red *(mixers).*

17 Fuente https://bitcoinfees.info/.

NÚMERO DE TRANSACCIONES DIARIAS GRÁFICO 3

FUENTE: https://www.blockchain.com.

Es cierto que pueden introducirse modificaciones para incrementar la capacidad de proceso de Bitcoin, la más inmediata de las cuales sería incrementar el tamaño máximo de los bloques. Sin embargo, no está claro que un sistema basado en una prueba de trabajo tan exigente como la que requiere Bitcoin pueda modificarse para procesar un volumen de operaciones significativamente mayor.

3.6 Eficiencia y modelo de negocio

El funcionamiento de Bitcoin depende de la existencia de mineros que incurran en un gasto (inversión en *hardware* y gasto de electricidad) para obtener ingresos a través de las comisiones por transacción y los *bitcoins* que se crean para recompensar al minero que resuelve el puzle criptográfico que permite crear el bloque. En principio, la dificultad de este problema criptográfico se ajusta automáticamente para que el ritmo de creación de bloques sea más o menos constante. A pesar de ciertas bajadas esporádicas, la complejidad muestra una tendencia creciente, evidenciando la competencia y la creciente especialización de los mineros. Esta especialización favorece la creación de *pools* o clubes de mineros que ponen en común sus recursos de computación para incrementar sus ganancias y reducir la variabilidad en la tasa de obtención de las recompensas. La agrupación en *pools* de mineros lleva a un proceso de centralización: en la actualidad, los cuatro principales *pools* de mineros reúnen más del 50 % del poder de computación de toda la red. Esto nos lleva a un modelo de negocio oligopolista en el que la fuerte inversión inicial en *hardware* especializado podría ser una barrera de entrada para nuevos actores. Este modelo está muy lejos de la descentralización con la que se suele caracterizar a Bitcoin.

Más allá del número de mineros, la complejidad del proceso criptográfico de validación y el gasto de recursos que lleva aparejada deberían ser suficientes para cuestionar la eficiencia de un sistema que procesa menos de 300.000 operaciones diarias. En agosto de 2018, algunas estimaciones apuntan a que el esquema Bitcoin consumía 73,12 TWh, una cantidad de energía

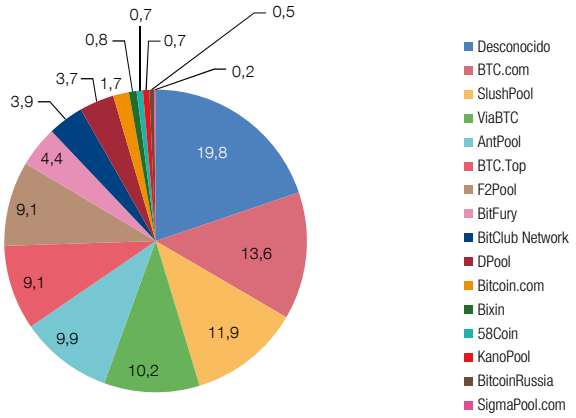
EVOLUCIÓN DE LA DIFICULTAD DE LA PRUEBA DE TRABAJO

GRÁFICO 4

FUENTE: https://www.blockchain.com.

CUOTA DE MERCADO DE LOS *POOLS* DE MINERÍA MÁS POPULARES (%)

GRÁFICO 5



FUENTE: www.blockchain.info.

similar a la de un país como Austria[18]. En un sistema centralizado basado en la confianza, un volumen semejante de transacciones se podría procesar con un consumo ínfimo de recursos en comparación con Bitcoin[19].

Este tremendo coste se cubre actualmente con las comisiones y con la emisión de nuevas monedas al crear bloques. A medida que las recompensas automáticas disminuyan y si la dificultad sigue en aumento[20], es previsible que las comisiones tiendan a aumentar para cubrir

18 Fuente: https://digiconomist.net/bitcoin-energy-consumption. Esta energía supone el 0,33 % del consumo mundial y sería suficiente para abastecer a más de 6,7 millones de hogares estadounidenses. Con la energía consumida para registrar una única transacción en Bitcoin se podría abastecer de electricidad a unos 31 hogares estadounidenses durante un día.

19 De acuerdo con los datos de https://digiconomist.net/bitcoin-energy-consumption, la energía consumida en la verificación de una transacción de Bitcoin sería suficiente para procesar más de medio millón de operaciones con tarjeta VISA.

20 En «Beyond the doomsday economics of «proof-of-work» in cryptocurrencies» se puede encontrar un análisis detallado de la viabilidad a largo plazo de Bitcoin.

el gran coste de electricidad del esquema, lo que podría poner en cuestión su viabilidad. A finales de 2018 se ha puesto de manifiesto como la volatilidad en los precios de los *bitcoins* puede provocar variaciones en el número de mineros. En este caso, el descenso de su contravalor en dólares ha provocado una disminución en el rendimiento obtenido por los mineros y su abandono en la actividad, lo que ha provocado a su vez la disminución en la generación de bloques y en consecuencia un ajuste a la dificultad.

3.7 Gobierno

Un aspecto esencial de Bitcoin (al que históricamente se le ha prestado menos atención que a sus características técnicas) es el de su gobierno. Normalmente se ha presentado a Bitcoin como un protocolo automático con reglas inmutables. Por ello, se le considera en ciertos círculos como más digno de confianza que una autoridad como un banco central, que puede actuar de forma discrecional decidiendo la tasa de creación de dinero y determinando qué transacciones han de ser aprobadas y cuáles no. Sin embargo, el esquema no es inmutable, sino que evoluciona lentamente siempre y cuando una masa crítica de usuarios se ponga de acuerdo para implantar los cambios. El tamaño máximo de los bloques o la regla que determina la creación de *bitcoins* a tasas decrecientes, por ejemplo, podrían cambiarse en cualquier momento si un número suficiente de usuarios se pusiesen de acuerdo para modificarlas. Un cambio significativo que fuese aceptado por una parte de la comunidad de usuarios pero no por otra llevaría a una bifurcación del sistema[21].

La ausencia de una autoridad central y la diversidad y falta de coordinación de los actores del sistema hacen que sea difícil llegar a acuerdos para mejorar gradualmente el sistema o reaccionar ante cambios imprevistos.

21 Precisamente el tamaño máximo de los bloques (uno de los aspectos más controvertidos de Bitcoin, puesto que este tamaño máximo incide directamente en la capacidad del sistema) ha sido el causante de la escisión de Bitcoin en dos esquemas incompatibles entre sí (Bitcoin y Bitcoin Cash) desde agosto de 2017. Hay muchas otras versiones de Bitcoin, aunque se suele reservar este nombre para la versión mayoritaria.

4 Conclusiones

Bitcoin se presenta como una alternativa al dinero y como un mecanismo de pagos más eficiente que los sistemas de pago tradicionales. Para evitar el coste que los intermediarios introducen en los sistemas de intercambio, Bitcoin persigue la creación de un mecanismo alternativo de pagos en el que no existen intermediarios que puedan censurar las transacciones (entendido como la capacidad de detenerlas o revertirlas).

Es fundamental resaltar el objetivo último del esquema, pues condiciona su diseño, que es una respuesta casi natural al objetivo perseguido [Brown (2016)]: teniendo en cuenta que queremos realizar pagos a distancia con un activo digital, necesitamos algún validador que evite que un usuario gaste varias veces los mismos saldos *(double spend)* y verifique la coherencia del historial de transacciones; puesto que no deseamos que una autoridad central pueda controlar el flujo de pagos, debemos establecer una red abierta en la que cualquiera pueda actuar como validador y el historial de transacciones sea público; dado que todas las transacciones son públicas, necesitamos que sean anónimas para garantizar la confidencialidad; para evitar que uno o varios validadores traten de falsificar el registro de transacciones, se requiere que realicen una prueba de trabajo de forma competitiva y para incentivar el coste de realizar la prueba de trabajo establecemos una recompensa en forma de nuevas unidades monetarias. Los detalles del funcionamiento de Bitcoin se pueden encontrar en el apartado 2, pero lo importante es resaltar que el diseño es coherente con el objetivo perseguido.

Bitcoin permite, pues, implantar un sistema de pagos sin censura, lo que constituye una innovación muy interesante que posibilita la resolución de un problema complejo, pero esto no implica necesariamente que el esquema sea un buen sistema de pago. Los numerosos defensores de Bitcoin arguyen que supone una mejora respecto a las operaciones de pago tradicionales a través del circuito bancario, pero estas supuestas ventajas de Bitcoin no parecen estar refrendadas por la información disponible en la actualidad

Todo apunta a que Bitcoin tiene graves carencias si se pretende utilizar como un sistema de pago a gran escala. El principal problema es que la ausencia de intermediarios y la consiguiente descentralización del sistema en un conjunto de validadores entre los que no existe confianza nos conducen a un proceso de validación intensivo en el consumo de recursos, lo que resta eficiencia al sistema. Dicho de otro modo, existe un claro *trade-off* entre el consumo de recursos asociado a la validación descentralizada de operaciones y la confianza: los sistemas centralizados con un intermediario en el que confían las partes permiten el diseño de sistemas mucho más simples y económicos.

No es de extrañar que Bitcoin tenga estos problemas. El esquema no fue diseñado como una alternativa a los sistemas de pago tradicionales, sino como un sistema de pago *en el que no hubiera una autoridad central con poder para autorizar o rechazar transacciones* (un sistema sin posibilidad de censura). Bitcoin es una solución imaginativa y elegante a este problema, pero este no es el problema que buscan resolver los sistemas de pago que utilizamos

habitualmente. Los sistemas de pago tradicionales tienen como objetivo facilitar el envío de dinero entre dos actores cualesquiera de la forma más sencilla posible, a un coste reducido, de forma rápida y con un alto grado de seguridad. Estos objetivos son muy diferentes, por lo que no es en absoluto sorprendente que Bitcoin no funcione de manera satisfactoria como sistema de pago (quizás lo sorprendente fuese lo contrario).

Los detractores de Bitcoin lo presentan en ocasiones como una «solución en busca de su problema», mientras que los partidarios de Bitcoin creen que es una solución a los (en su opinión) problemas del dinero fiduciario y los sistemas de pago tradicionales. En realidad, Bitcoin parece ser la solución a un problema, pero a un problema diferente del que normalmente mencionan sus partidarios: la creación de un sistema sin censura. Teniendo en cuenta que para la mayor parte de los agentes la existencia de intermediarios de confianza no es un problema, así como los costes e ineficiencias que se generan al tratar de eliminar a estos intermediarios, no parece que Bitcoin, en su configuración actual, vaya a tener un impacto significativo para el sector financiero como un sistema de pago alternativo a los canales tradicionales.

Bibliografía

BANCO DE ESPAÑA (2018). *Memoria anual sobre la vigilancia de las infraestructuras de los mercados financieros, 2017.*

BANK OF INTERNATIONAL SETTLEMENTS (2019). *Beyond the doomsday Economics of "proof-of-work" in cryptocurrencies.* https://www.bis.org/publ/work765.pdf.

BROWN, R. G. (2016). *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services* (https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/).

HALABURDA, H., y M. SARVARY (2016). *Beyond Bitcoin: The economics of digital currencies,* Palgrave MacMilllan.

https://bitcoinfees.info/.

NAKAMOTO, S. (2008). «Bitcoin: a peer-to-peer electronic cash system».

NAYARANAN, A., J. BONNEAU, E. FELTEN, A. MILLER y S. GOLDFEDER (2016). *Bitcoin and cryptocurrency technologies.*

NIELSEN, M. (2013). *How the Bitcoin protocol actually Works* (http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/).

www.Blockchain.com.

PUBLICACIONES DEL BANCO DE ESPAÑA

DOCUMENTOS OCASIONALES

1201 ELOÍSA ORTEGA y JUAN PEÑALOSA: Claves de la crisis económica española y retos para crecer en la UEM. (Existe una versión en inglés con el mismo número).
1202 MARÍA J. NIETO: What role, if any, can market discipline play in supporting macroprudential policy?
1203 CONCHA ARTOLA y ENRIQUE GALÁN: Las huellas del futuro están en la web: construcción de indicadores adelantados a partir de las búsquedas en Internet. (Existe una versión en inglés con el mismo número).
1204 JOSÉ LUIS MALO DE MOLINA: Luis Ángel Rojo en el Banco de España.
1205 PABLO HERNÁNDEZ DE COS y CARLOS THOMAS: El impacto de la consolidación fiscal sobre el crecimiento económico. Una ilustración para la economía española a partir de un modelo de equilibrio general.
1206 GALO NUÑO, CRISTINA PULIDO y RUBÉN SEGURA-CAYUELA: Long-run growth and demographic prospects in advanced economies.
1207 IGNACIO HERNANDO, JIMENA LLOPIS y JAVIER VALLÉS: Los retos para la política económica en un entorno de tipos de interés próximos a cero.
1208 JUAN CARLOS BERGANZA: Fiscal rules in Latin America: a survey.
1209 ÁNGEL ESTRADA y EVA VALDEOLIVAS: The fall of the labour income share in advanced economies.
1301 ETTORE DORRUCCI, GABOR PULA y DANIEL SANTABÁRBARA: China's economic growth and rebalancing.
1302 DANIEL GARROTE, JIMENA LLOPIS y JAVIER VALLÉS: Los canales del desapalancamiento del sector privado: una comparación internacional.
1303 PABLO HERNÁNDEZ DE COS y JUAN F. JIMENO: Fiscal policy and external imbalances in a debt crisis: the Spanish case.
1304 ELOÍSA ORTEGA y JUAN PEÑALOSA: Algunas reflexiones sobre la economía española tras cinco años de crisis. (Existe una versión en inglés con el mismo número).
1401 JOSÉ MARÍA SERENA y EVA VALDEOLIVAS: Integración financiera y modelos de financiación de los bancos globales.
1402 ANTONIO MONTESINOS, JAVIER J. PÉREZ y ROBERTO RAMOS: El empleo de las administraciones públicas en España: caracterización y evolución durante la crisis.
1403 SAMUEL HURTADO, PABLO MANZANO, EVA ORTEGA y ALBERTO URTASUN: Update and re-estimation of the Quarterly Model of Banco de España (MTBE).
1404 JUAN CARLOS BERGANZA, IGNACIO HERNANDO y JAVIER VALLÉS: Los desafíos para la política monetaria en las economías avanzadas tras la Gran Recesión.
1405 FERNANDO LÓPEZ VICENTE y JOSÉ MARÍA SERENA GARRALDA: Macroeconomic policy in Brazil: inflation targeting, public debt structure and credit policies.
1406 PABLO HERNÁNDEZ DE COS y DAVID LÓPEZ RODRÍGUEZ: Estructura impositiva y capacidad recaudatoria en España: un análisis comparado con la UE. (Existe una versión en inglés con el mismo número).
1407 OLYMPIA BOVER, ENRIQUE CORONADO y PILAR VELILLA: The Spanish survey of household finances (EFF): description and methods of the 2011 wave.
1501 MAR DELGADO TÉLLEZ, PABLO HERNÁNDEZ DE COS, SAMUEL HURTADO y JAVIER J. PÉREZ: Los mecanismos extraordinarios de pago a proveedores de las Administraciones Públicas en España. (Existe una versión en inglés con el mismo número).
1502 JOSÉ MANUEL MONTERO y ANA REGIL: La tasa de actividad en España: resistencia cíclica, determinantes y perspectivas futuras.
1503 MARIO IZQUIERDO y JUAN FRANCISCO JIMENO: Employment, wage and price reactions to the crisis in Spain: Firm-level evidence from the WDN survey.
1504 MARÍA DE LOS LLANOS MATEA: La demanda potencial de vivienda principal.
1601 JAVIER MENCÍA y JESÚS SAURINA: Política macroprudencial: objetivos, instrumentos e indicadores. (Existe una versión en inglés con el mismo número).
1602 LUIS MOLINA, ESTHER LÓPEZ y ENRIQUE ALBEROLA: El posicionamiento exterior de la economía española.
1603 PILAR CUADRADO y ENRIQUE MORAL-BENITO: El crecimiento potencial de la economía española (Existe una versión en inglés con el mismo número).
1604 HENRIQUE S. BASSO y JAMES COSTAIN: Macroprudential theory: advances and challenges.
1605 PABLO HERNÁNDEZ DE COS, AITOR LACUESTA y ENRIQUE MORAL BENITO: An exploration of real-time revisions of output gap estimates across European countries.
1606 PABLO HERNÁNDEZ DE COS, SAMUEL HURTADO, FRANCISCO MARTÍ y JAVIER J. PÉREZ: Public finances and inflation: the case of Spain.

1607 JAVIER J. PÉREZ, MARIE AOURIRI, MARÍA M. CAMPOS, DMITRIJ CELOV, DOMENICO DEPALO, EVANGELIA PAPAPETROU, JURGA PESLIAKAITĖ, ROBERTO RAMOS y MARTA RODRÍGUEZ-VIVES: The fiscal and macroeconomic effects of government wages and employment reform.

1608 JUAN CARLOS BERGANZA, PEDRO DEL RÍO y FRUCTUOSO BORRALLO: Determinants and implications of low global inflation rates.

1701 PABLO HERNÁNDEZ DE COS, JUAN FRANCISCO JIMENO y ROBERTO RAMOS: El sistema público de pensiones en España: situación actual, retos y alternativas de reforma. (Existe una versión en inglés con el mismo número).

1702 EDUARDO BANDRÉS, MARÍA DOLORES GADEA-RIVAS y ANA GÓMEZ-LOSCOS: Regional business cycles across Europe.

1703 LUIS J. ÁLVAREZ e ISABEL SÁNCHEZ: A suite of inflation forecasting models.

1704 MARIO IZQUIERDO, JUAN FRANCISCO JIMENO, THEODORA KOSMA, ANA LAMO, STEPHEN MILLARD, TAIRI RÕÕM y ELIANA VIVIANO: Labour market adjustment in Europe during the crisis: microeconomic evidence from the Wage Dynamics Network survey.

1705 ÁNGEL LUIS GÓMEZ y M.ª DEL CARMEN SÁNCHEZ: Indicadores para el seguimiento y previsión de la inversión en construcción.

1706 DANILO LEIVA-LEON: Monitoring the Spanish Economy through the Lenses of Structural Bayesian VARs.

1707 OLYMPIA BOVER, JOSÉ MARÍA CASADO, ESTEBAN GARCÍA-MIRALLES, JOSÉ MARÍA LABEAGA y ROBERTO RAMOS: Microsimulation tools for the evaluation of fiscal policy reforms at the Banco de España.

1708 VICENTE SALAS, LUCIO SAN JUAN y JAVIER VALLÉS: The financial and real performance of non-financial corporations in the euro area: 1999-2015.

1709 ANA ARENCIBIA PAREJA, SAMUEL HURTADO, MERCEDES DE LUIS LÓPEZ y EVA ORTEGA: New version of the Quarterly Model of Banco de España (MTBE).

1801 ANA ARENCIBIA PAREJA, ANA GÓMEZ LOSCOS, MERCEDES DE LUIS LÓPEZ y GABRIEL PÉREZ QUIRÓS: A short-term forecasting model for the Spanish economy: GDP and its demand components.

1802 MIGUEL ALMUNIA, DAVID LÓPEZ-RODRÍGUEZ y ENRIQUE MORAL-BENITO: Evaluating the macro-representativeness of a firm-level database: an application for the Spanish economy.

1803 PABLO HERNÁNDEZ DE COS, DAVID LÓPEZ RODRÍGUEZ y JAVIER J. PÉREZ: Los retos del desapalancamiento público. (Existe una versión en inglés con el mismo número).

1804 OLYMPIA BOVER, LAURA CRESPO, CARLOS GENTO y ISMAEL MORENO: The spanish survey of household finances (EFF): Description and methods of the 2014 wave.

1805 ENRIQUE MORAL-BENITO: The microeconomic origins of the Spanish boom.

1806 BRINDUSA ANGHEL, HENRIQUE BASSO, OLYMPIA BOVER, JOSÉ MARÍA CASADO, LAURA HOSPIDO, MARIO IZQUIERDO, IVAN A. KATARYNIUK, AITOR LACUESTA, JOSÉ MANUEL MONTERO y ELENA VOZMEDIANO: La desigualdad de la renta, el consumo y la riqueza en España. (Existe una versión en inglés con el mismo número).

1807 MAR DELGADO-TÉLLEZ y JAVIER J. PÉREZ: Institutional and economic determinants of regional public debt in Spain.

1808 CHENXU FU y ENRIQUE MORAL-BENITO: The evolution of Spanish total factor productivity since the Global Financial Crisis.

1809 CONCHA ARTOLA, ALEJANDRO FIORITO, MARÍA GIL, JAVIER J. PÉREZ, ALBERTO URTASUN y DIEGO VILA: Monitoring the Spanish economy from a regional perspective: main elements of analysis.

1810 DAVID LÓPEZ-RODRÍGUEZ y CRISTINA GARCÍA CIRIA: Estructura impositiva de España en el contexto de la Unión Europea.

1811 JORGE MARTÍNEZ: Previsión de la carga de intereses de las Administraciones Públicas.

1901 CARLOS CONESA: Bitcoin: ¿una solución para los sistemas de pago o una solución en busca de problema?

BANCO DE **ESPAÑA**
Eurosistema

Unidad de Servicios Auxiliares
Alcalá, 48 - 28014 Madrid
Correo electrónico: publicaciones@bde.es
www.bde.es