novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*), representa a España en **IFIP** (*International Federation for Information Processing*) y es miembro de **CLEI** (*Centro Latinoamericano de Estudios de Informática*) y de **CECUA** (*Confederation of European Computer User Associations*). Asimismo tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*) y colabora con diversas asociaciones informáticas españolas.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Gutierre de Cetina 24, 28017 Madrid •Tlfn.914029391 <novatica@ati.es>
Administración y Redacción ATI Cataluña
Calle Ávila 50, 3a planta, local 9, 08005 Barcelona
Tlfn.934125235 <secregen@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Gutierre de Cetina 24, 28017 Madrid
Tlnf.914029391 <novatica@ati.es>
Imprenta: Impresión Offset Derra S.L., Llull 41, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: "El guardián" - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 238, noviembre 2016 - febrero 2017, año XLII

Monografía del próximo número: "Salud y tecnología"

Roberto José Fernández García
Ejecutivo de Cuentas en Telefónica; Estudiante de doctorado; Socio sénior de ATI

<rfernandez.casa@gmail.com>

El éxito de Bitcoin: La economía de la deep web

Resumen: *Bitcoin empezó con idea de desarrollar un proyecto de software libre que permitiese el funcionamiento de una moneda sustentada de manera colectiva por la red, permitiendo hacer pagos instantáneos a cualquier parte del mundo sin intermediarios. Se trata una divisa descentralizada que opera a través de tecnología P2P. Al no existir una autoridad central ni intermediación de ninguna institución financiera, los encargados de la gestión de las transacciones y de la creación del dinero son los propios usuarios de Bitcoin. Pero la no adopción del dinero virtual, Bitcoin por ejemplo, por parte de los bancos centrales mundiales se justifica por los lentos procesos de regulación y los escasos incentivos al cambio. Los bancos centrales inciden en los casos de financiación de actividades ilícitas, blanqueo de capitales, etc. para tirar por tierra la propuesta. Ha sido Japón, quien en febrero de 2016 ha considerado a Bitcoin como una divisa corriente (en vez de mercancía) volviendo a situarse a la vanguardia de la regulación de las divisas digitales. Aunque la imagen de Bitcoin ha sufrido por ser la moneda empleada en Silk Road y por la bancarrota de su principal agencia de cambio, Mt. Gox, hoy cotiza por encima de los 420$ y su futuro se presenta halagüeño. El dinero electrónico sólo está empezando pero parte con muchos intereses creados ¿hasta cuándo las resistencias al cambio?*

Palabras clave: *Bitcoin, dinero electrónico, Mt.Gox, Ruta de la Seda, Satoshi Nakamoto, web profunda*.

1. Introducción

En los últimos años, el incremento de ancho de banda en las comunicaciones, la capacidad de los dispositivos móviles, el desarrollo masivo de aplicaciones, el crecimiento vertiginoso de las comunidades virtuales, la compartición de conocimiento, etc. han desembocado en una economía conducida a través de Internet. Actualmente, programas "robots" o "*bots*" escuchan las tendencias bursátiles con el fin de realizar operaciones automáticas y muy rápidas a nivel mundial.

En este entorno donde van surgiendo nuevos modelos de negocio *e-Business*, se ha hecho necesaria una divisa virtual y descentralizada para pagos instantáneos, intercambio de bienes y servicios, etc., y con costos de transacción mínimos.

Esta divisa no dispone de una autoridad central o intermediación de una institución financiera, por lo que son sus propios usuarios colectivamente, la red abierta P2P (*peer to peer*), los encargados de la gestión de las transacciones y de la creación de dinero. Bitcoin (BTC) es el tipo de divisa más generalizado, aunque existen otras.

Por otra parte, la *Deep Web*, el lado oscuro de Internet, es una red de webs de no fácil acceso al usuario común, donde pululan todo tipo de *hackers*, agentes del gobierno, altos cargos militares y las peores lacras de la sociedad. Para entender la *Deep Web* o "web profunda" [1] lo primero que debemos saber es que las páginas que todo el mundo visita día a día: Google, Wikipedia, Amazon y tantas otras, pertenecen a la *surface web* o "web superficial".

En la *Deep Web* se puede encontrar información que roza la ilegalidad o bien es completamente ilegal, páginas, foros, *wikis*, manuales, anuncios y artículos sobre: venta de órganos, venta de drogas, venta de armas, compra de artículos robados, *hackers*, contratación de sicarios, *ebooks* de todo tipo, pedofilia, necrofilia, zoofilia, violación y demás parafilias, canibalismo, guerrillas, asesinatos, secretos corporativos, documentos clasificados de empresas o gobiernos, terrorismo mundial, tráfico de seres humanos y un gran etcétera.

El caso de éxito "Silk Road" (La Ruta de la Seda) [2] ofrecía, través de la red anónima TOR, una plataforma para la venta de narcóticos en línea, realizando transacciones por medio de *bitcoins* (ver **figura 1**).

Era la web más grande de su tipo, llegando a facturar millones de dólares cada mes. El FBI encontró a su fundador, Ross Ulbricht, lo capturó y dejó el sitio cerrado.

2. Dinero electrónico

2.1. Historia del dinero

El dinero se intercambia en transacciones para compras de bienes y servicios, facilitando el comercio de un bien por otro. Un buen dinero debe ser transportable, divisible (las fracciones de bitcoins se denominan *satoshis*), corriente, escaso (tendiendo a una cota máxima: 21 millones en el caso de bitcoins) y no necesita tener valor intrínseco. El valor de cada unidad de dinero se determina por el equilibrio entre la oferta y la demanda.

El dinero puede ser físico (oro, plata, platino, monedas/billetes, perlas, etc.), electrónico (PayPal, WebMoney, e-gold, etc.), o virtual (Bitcoin, Litecoin, etc.).

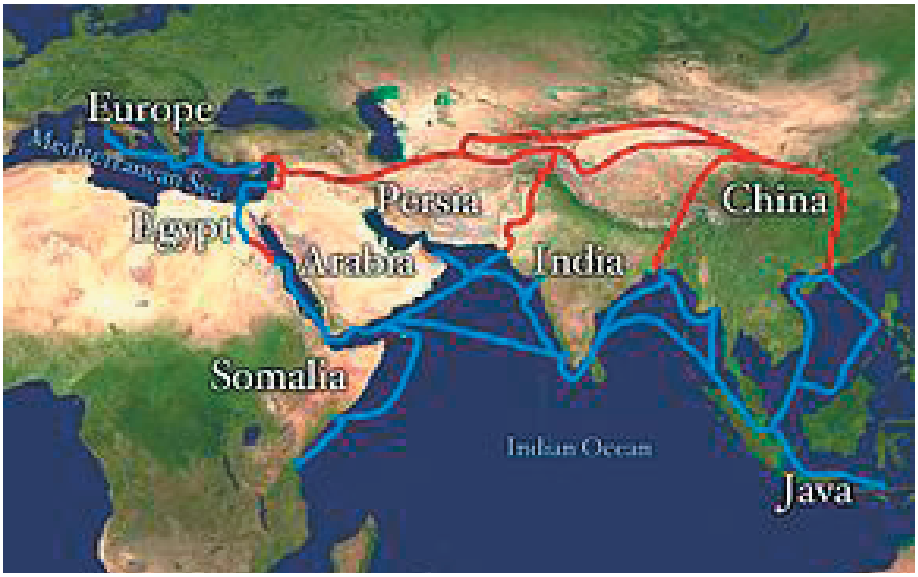

Figura 1. La Ruta de la Seda. Fuente: Wikipedia [3].

> “ En este entorno donde van surgiendo nuevos modelos de negocio *e-Business*, se ha hecho necesaria una divisa virtual y descentralizada para pagos instantáneos, intercambio de bienes y servicios, etc., y con costos de transacción mínimos ”

El dinero presenta propiedades como las siguientes:

- Es una unidad de cuenta con valor definido; en Bitcoin quizás con alta variabilidad.
- Es un medio de intercambio.
- Es un almacén de valor no perecedero.
- Es difícil de falsificar.
- Permite transacciones rápidas.
- Previene el doble gasto (Se han constatado casos en transacciones rápidas con bitcoins).
- Permite cierto grado de anonimato. Bitcoin lo permite.

2.2. Aspectos técnicos e institucionales

Según el Banco de España, se entiende por dinero electrónico [4] el valor monetario representado por un crédito exigible a su emisor:

a) Almacenado en un soporte electrónico.
b) Emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido.
c) Aceptado como medio de pago por empresas distintas del emisor.

El dinero electrónico ha tenido que dar solución a los siguientes cinco puntos:

1) Implantación técnica. Productos basados: bien en software, utilizando un cliente específico para PC, *smartphone*, etc. (sistemas *software-based*: Paypal o pagos a través del teléfono móvil: Telefónica-BBVA) o bien en hardware, incluyendo un chip en una tarjeta de plástico (VISA Cash, Blue American Express).
2) Requisitos institucionales. Habitualmente en una transacción con dinero electrónico encontraremos cuatro agentes prestadores de servicio: el proveedor del dinero electrónico, la red de operadores, los vendedores de hardware y software especializado y los encargados de compensar las transacciones con dinero electrónico[1].

Desde el punto de vista normativo, los proveedores son el elemento más importante, ya que el dinero electrónico supone un pasivo en sus balances. Por el contrario, los operadores y vendedores no son más que proveedores en el ámbito técnico. Finalmente, la compensación la llevan a cabo bancos o compañías especializadas.

3) Método de transferencia de valor. Tradicionalmente, sólo eran permitidos los pagos de consumidor a proveedor, hoy es posible realizar transacciones P2P[2] en las que el propio sistema consolida la transacción.
4) Registro de las transferencias. En la mayoría de los casos, las operaciones se registran en una central de base de datos controlada. En el caso de operaciones P2P, sólo se grabarán y podrán ser controladas si el consumidor contacta con su operador de dinero electrónico.
5) Divisa de valor almacenado. Antiguamente, en la mayoría del dinero electrónico, el valor guardado sólo figuraba en la moneda nacional. En la actualidad, es posible pagar y registrar el valor almacenado en diferentes divisas, entre ellas Bitcoin.

2.3. Aspectos regulatorios

Cuando el Tribunal de Justicia de la Unión Europea decidió que el Bitcoin era una moneda más, hubo cierta esperanza de que quedara fuera de las manos de nuestros gobernantes.

Pero la Unión Europea quiere controlar las criptomonedas, con el argumento del terrorismo. El problema es que técnicamente no hay forma de controlarlas, así que la única regulación posible es prohibirlas y combatir su uso:

- No permitir a los comercios aceptarlas.
- Intentar identificar a las personas que las usan.

Bitcoin permite cierto anonimato (aunque las transacciones son públicas) y eso pone en riesgo los controles de capitales. Si se sigue extendiendo su uso parece seguro que la Unión Europea va a intervenir fiscalizando las transacciones financieras.

Los principales problemas de carácter regulatorio para la adopción del dinero electrónico son los siguientes:

1) Un lento proceso de regulación. La aparición de nuevos sistemas de pago guarda una estrecha relación con la política monetaria, pero no debe suponer un riesgo para el consumidor. Por este motivo, el marco legal y reglamentario debe evolucionar en el mismo sentido y celeridad: prevaleciendo la protección al consumidor y garantizado la viabilidad del sistema de pagos en el futuro.
2) Necesidad de una coordinación internacional. Los nuevos sistemas, especialmente los basados en software, no requieren de ninguna base geográfica, lo que aumenta considerablemente los riesgos.

La Unión Europea ya ha empezado a legislar para garantizar la viabilidad y la seguridad de los medios de pago del futuro. La Directiva Comunitaria 2000/46 establece que estas instituciones serán tratadas como entidades de crédito en lo que a exigencias de reservas mínimas y tendrán acceso a la refinanciación ofrecida por el Banco Central.

Desde 2011, en España su regulación está contenida en la Ley 21/2011, de 26 de julio, de dinero electrónico.

3) Pocos incentivos para el cambio, ya que aún es necesario disponer de dinero tradicional para efectuar compras en el mundo real. El dinero electrónico se parece a las tarjetas prepago, en las que el usuario debe poner dinero en una tarjeta con un chip integrado antes de poder utilizarla para pagar.

Las entidades de dinero electrónico, conocidas como EDE, están reguladas en el Ley 21/2011. Estas entidades se dedican a emitir dinero electrónico que es admitido como medio de pago por empresas distintas a la entidad emisora. Una de las entidades más conocidas es Paypal.

Además de las entidades bancarias existen dos EDE’s en España, [5] (MoneyToPay y YoUnique Money) que, junto con otras autorizadas en la Unión Europea, pueden operar en España.

> “Con Bitcoin no hay entidades en las que confiemos. No hay un banco que nos asegure que ‘este dinero es real’. En su lugar, la validez de Bitcoin reside en su tecnología, en todas las técnicas que aseguran que funciona como si fuese una moneda real”

3. El Bitcoin

3.1. Nacimiento e historia

Internet ha transformado muchas cosas, y una de ellas es nuestra forma de ver el dinero. Éste ha pasado de ser algo físico a ser un bien intangible, un número en una página. Creemos que está ahí porque confiamos en la entidad emisora y sabemos que lo gestionan como si fuese dinero físico y tangible.

Con Bitcoin no hay entidades en las que confiemos. No hay un banco que nos asegure que “este dinero es real”. En su lugar, la validez de Bitcoin reside en su tecnología, en todas las técnicas que aseguran que funciona como si fuese una moneda real.

La idea pionera de David Chaum data de 1982, con el desarrollo *e-cash*, y fue en 2007 cuando Satoshi Nakamoto concibió Bitcoin con el objeto de desarrollar un proyecto de software libre que permitiese el funcionamiento de una moneda sustentada de manera colectiva por la red y que permitiera pagos instantáneos a cualquier parte del mundo sin intermediarios.

La/s identidad/es bajo el seudónimo de Satoshi Nakamoto son todo un misterio. Se cree que el nombre fuese creado expresamente para el proyecto con la finalidad de proteger la verdadera identidad/es del autor/es y la red Bitcoin. Empezó a trabajar en el proyecto en 2007, para ir reduciendo su participación en 2009 y desaparecer en 2010.

3.2. Diferencias entre dinero electrónico y dinero virtual

El dinero virtual, como Bitcoin, puede considerarse un tipo específico de dinero electrónico utilizado para transacciones en el ciberespacio [6].

El Banco Central Europeo establece similitudes y diferencias entre el dinero electrónico y el dinero virtual en cuanto a:

- Formato del dinero: ambos son digitales.
- Supervisión: el dinero electrónico sí lo tiene, mientras que el dinero virtual no.
- Tipos de riesgo: el dinero electrónico presenta principalmente riesgos operacionales mientras que en el dinero virtual los riesgos son legales, de crédito, de liquidez y operacionales.
- Estatus legal, el dinero electrónico está regulado, mientras que el dinero virtual no lo está.
- Unidad de cuenta, el dinero electrónico es dinero tradicional (euros, dólares, etc.) con estatus de moneda de curso legal, mientras que el dinero virtual es dinero criptográfico inventado (bitcoins) sin estatus de moneda de curso legal.
- Aceptación: el dinero electrónico es por compromiso del expendedor, mientras que el dinero virtual se utiliza dentro de una comunidad virtual específica.
- Expendedor: el dinero electrónico lo establece legalmente una institución de dinero electrónico (VISA o MasterCard), mientras que el dinero virtual surge a través de estructuras descentralizadas abiertas, de software libre, no financieras.
- Canjear fondos: El dinero electrónico está garantizado (por valor), mientras que el dinero virtual no está garantizado.
- Suministro: en el dinero electrónico está fijado, mientras que en el dinero virtual no lo está, depende de las decisiones del expendedor.

3.3. Aspectos teóricos y prácticos en relación con el dinero virtual

Bitcoin/BTC puede considerarse bajo tres prismas:

1) Moneda virtual o forma innovadora de establecer dinero digital a través de Internet. Con un sistema de pago de código abierto, basado en una red P2P abierta, descentralizado, que utiliza transacciones irrevocables y fundamentado en *Proof-of-Work*/PoW.
2) Un nuevo tipo de sistema de pago o medio de intercambio privado virtual basado en PoW, persona a persona, que no necesita ni de autoridad-banco central, ni de expedidor, ni de sistema de reserva que controle el suministro de BTCs, ni de terceras partes de confianza o TTP para posibilitar o supervisar las transacciones *online*.
3) Protocolo criptográfico para procesos financieros en nuevos modelos de *e-Business* y *e-Commerce*, con un crecimiento importante en el área de la criptografía financiera.

Tal y como funciona BTC [7], el envío es instantáneo y toda operación puede ser monitorizada en tiempo real.

Para hacer uso de Bitcoin necesitaremos descargarnos un cliente de software libre que contiene: pares de claves para cada dirección, transacciones desde o hacia tus direcciones, las preferencias del usuario, etc.
El cliente se podrá descargar en:

1) PCs/Macs (Bitcoinqt, Armony, Bitcoinspinner, etc.). Proporcionan control total de su monedero, y exigen hacer copias de seguridad y proteger el dinero.
2) Móviles (Coinbase, Bitcoin-wallet, etc.). Permiten tener bitcoins en el bolsillo, se puede pagar o intercambiar monedas escaneando un código óptico QR o utilizando tecnología RF NFC (a través de un *smartphone* o *smartcard*).
3) Monederos web. Permiten utilizar bitcoins en cualquier lugar. Se debe elegir un proveedor de servicios de monedero web para almacenar sus bitcoins. Para aceptar bitcoins se necesita poner la dirección BTC en el sitio web.

3.4. Implementación técnica

La compleja tecnología de Bitcoin *garantiza que se pueda usar como moneda* sin que cualquiera pueda crear dinero, asegurando que sólo puedes gastar tu dinero una vez, y controlando la introducción de nuevas monedas en el mercado.

Esta completa tecnología comienza por la definición técnica de dos términos: *Hash y firma digital*.

En el caso de Bitcoin, el algoritmo es SHA256. Definimos *hash* como un objeto (cadena de texto, número,… representado en bits) de *identificación única y constante,* como nuestra huella dactilar. Tiene la peculiaridad de que es una función “de una vía”, desde el objeto es muy fácil obtener su *hash* y si tienes el *hash* es extremadamente difícil obtener el objeto original del que proviene.

> “La compleja tecnología de Bitcoin *garantiza que se pueda usar como moneda* sin que cualquiera pueda crear dinero, asegurando que sólo puedes gastar tu dinero una vez, y controlando la introducción de nuevas monedas en el mercado”

Firma digital:. Bitcoin utiliza ECDSA, firma digital de curva elíptica. La firma digital certifica que eres tú quien ha creado, verificado, o aceptado ese objeto. Para ello se usan dos claves: pública y privada. La clave privada se “combina” con el mensaje a firmar y se obtiene la firma.

Para verificar la firma, se “combina” la clave pública del firmante con la firma, que debería dar como resultado el mensaje original.

3.4.1. Las bases: transacciones y bloques

Una transacción es el envío de bitcoins de un usuario a otro, que tiene entrada y salida: de donde viene el dinero y a dónde va. Su ID (identificación) es un *hash* combinado del ID de las entradas y del ID del destinatario (su clave pública).

Así se fija de forma inequívoca quién es el destinatario y de dónde han salido las monedas. Después, ese ID se firma con la clave privada del emisor de la transferencia, quedando certificado que el dinero lo ha transferido su propietario.

Las transferencias *se agrupan en bloques,* que además contienen: un sello de tiempo, un número de verificación y el ID del bloque anterior. De esta forma, se genera una cadena de bloques (*Blockchain*), con toda la historia de transferencias de bitcoins (ver **figura 2**).

Los bloques los generan los *mineros*, y antes de crearlos verifican la validez de todas las transferencias (evitar que un usuario transfiera más de una vez la misma divisa). Una transferencia que se ha quedado fuera de la cadena de bloques no es válida, y del mismo modo una transferencia dentro de la cadena se considera válida sin más operaciones.

Cuando un nodo genera un bloque, lo emite al resto de nodos. Éstos verifican que el bloque esté construido correctamente y que sus transferencias sean válidas. Si el bloque es correcto, empezarán a trabajar con ese nuevo bloque como el final de la cadena.

Puede ocurrir que haya *dos ramas de la cadena*: un nodo ha emitido un bloque y en el mismo momento otro nodo ha emitido otro bloque distinto. En este caso, se conservan las dos ramas hasta que una de ellas sea más larga: ésta será la que se mantenga, y la otra se desechará.

Lo indicado funcionaría si todos los nodos que están creando bloques fuesen honestos. Pero sabemos que un nodo malicioso podría crear un bloque con una transferencia inválida (con dinero gastado dos veces) y después generar más bloques de forma masiva.

Al generar bloques válidos rápidamente, la transferencia inválida queda enterrada en la cadena. Cuando el resto de los nodos reciban esta cadena, que será la más larga de todo el entorno, verificarán como mucho los últimos bloques, darán la rama como válida y *esa transacción inválida pasará desapercibida*.

Es por esto que se hace necesario desarrollar un método que evite la generación de bloques indiscriminadamente y que obligue a los nodos a invertir tiempo en generar el bloque.

Este método se llama *proof-of-work* y consiste en encontrar el número de verificación, *nonce,* de tal forma que el *hash* del bloque sea menor que un determinado valor objetivo. El algoritmo búsqueda de ese número es prueba y error: empezamos en cero y calculamos el *hash*. Si es menor que el objetivo, perfecto, lo hemos encontrado. Si no, aumentamos en uno el *nonce* y volvemos a verificar. La probabilidad de encontrar un *nonce* válido es de $1/(2*10^{16})$. El valor objetivo se elige de tal forma que se tarde unos 10 minutos en generar un bloque. De esta forma, no pueden generar bloques rápidamente para ocultar transacciones.

El siguiente obstáculo es *el espacio de almacenamiento de toda la historia de transacciones:* guardar toda la cadena de bloques sin desperdiciar disco.

Para verificar una transacción, tenemos que comprobar que las entradas de monedas ya han sido verificadas. Normalmente, los clientes verifican varias transacciones atrás y consideran que el resto son válidas.

Es decir, se necesita una forma de guardar las transacciones y comprobar que están en los bloques: cada bloque contiene el *hash* combinado de las transferencias. Verificarlo es tan sencillo como coger el *hash* de la transferencia a verificar, combinarla con el resto de *hashes* de las transferencias del bloque y comprobar que tenemos la misma salida.

El problema surge cuando mantenemos muchas transferencias que no nos sirven para nada. Supongamos que, en un bloque, se ha gastado y verificado el dinero de todas las transferencias menos una. No vamos a necesitar el resto para verificar nada porque no vamos a llegar a tanta profundidad en la cadena. Sin embargo, tenemos que mante-

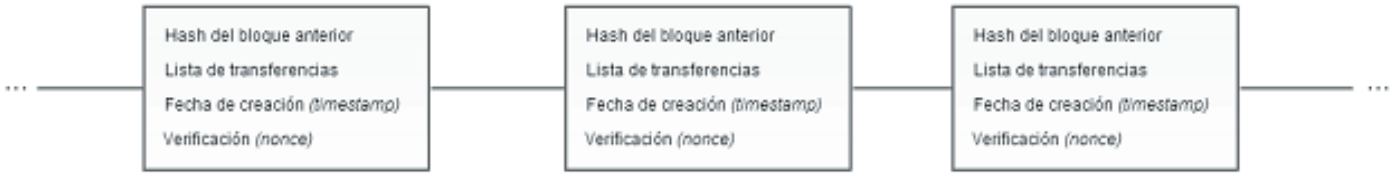

Figura 2. Cadena de bloques. Fuente: Wikimedia Commons.

> “ Cuando un nodo genera un bloque, lo emite al resto de nodos. Éstos verifican que el bloque esté construido correctamente y que sus transferencias sean válidas. Si el bloque es correcto, empezarán a trabajar con ese nuevo bloque como el final de la cadena ”

nerlas para que al verificar esa transferencia que no ha sido gastada, el *hash* siga siendo el mismo.

La solución pasa por usar un árbol de *hashes* o un árbol Merkle. Los *hashes* de las transferencias se van combinando dos a dos en forma de árbol binario. Así, cuando no necesitamos dos hermanos (comparten el mismo padre), podemos borrarlos y quedarnos con el nodo padre sin perder la posibilidad de verificar el resto de nodos del árbol. Esto reduce considerablemente el espacio necesario y permite quedarnos sólo con las transferencias más recientes y olvidarnos del resto.

En la **figura 3** podemos ver el funcionamiento de un árbol *hash*. Los recuadros verdes son los *hashes* que generamos, y los grises los que guardamos. Los sombreados no los usamos, así que no hace falta guardarlos.

3.4.2. Generación/minado de bitcoins

BTC es una moneda sin una entidad central que controle la inflación ni la generación de más dinero en el mercado. Será nuevamente la técnica la encargada de controlar la generación de monedas (con equipos específicos para ese propósito y varios procesadores gráficos o GPUs).

Cuando un nodo crea un bloque, además de todas las transferencias que haya verificado incluye otra más: una transferencia sin entradas. Cada vez que se verifica un bloque, se introducen nuevas monedas en el sistema. La tasa a la que se liberan nuevos BTC’s está controlada de tal forma que cada 4 años se reduce en el 50%. Así, está calculado que el número de BTC’s nunca pasará de los 21 millones.

Esto es un incentivo para los nodos de la red: cuantos más bloques verifiquen, más BTC’s ganan. Este enfoque hace más rentable ser un nodo honesto que uno malicioso.

Finalmente permite controlar el aspecto de “escasez” como requisito para considerar una divisa como BTC’s.

3.5. Ventajas e inconvenientes de la utilización de bitcoins

El principal reclamo de Bitcoin es su absoluta independencia con respecto al Estado o institución financiera. Al no estar sujeto a legislaciones nacionales, el uso de esta moneda como fondo para tus ahorros puede ser conveniente para evitar corralitos o devaluación de la moneda.

Las principales ventajas son las siguientes: [8]:

Permite el intercambio libre de dinero a nivel mundial simplemente con un equipo conectado a Internet.

- La identidad del usuario puede permanecer en todo momento en el anonimato. La dirección se genera aleatoriamente y no está ligada a ningún dato personal.
- Las transacciones son completamente públicas. Disponemos de webs donde puedes ver los movimientos en tiempo real o hacer seguimiento de una cuenta concreta. Por ejemplo: <https://www.biteasy.com>.
- Debido a que los pagos tienen un carácter irreversible, la reputación de los usuarios es algo básico para generar confianza a la hora de operar.
- Seguridad: En una transacción entre A y B, el cifrado con la clave pública asegura que B es el destinatario de la misma, y la firma con la clave privada, asegura que A es el emisor. El resto de los nodos de la red validan las firmas criptográficas y el valor de la transacción antes de aceptarla.
- Crecimiento sostenido. La oferta de bitcoins se limitará en el tiempo hasta un total de 21 millones. En 2033 se habrán generado casi todos los que van a estar en circulación (ver **figura 4**). Este límite no puede ser superado y el ritmo de creación no puede ser incrementado.
- Moneda descentralizada. No hay una autoridad central que la controle, es decir, ninguna institución o estado puede generar BTCs. Algo que sí hacen los bancos centrales con sus monedas, provocando procesos inflacionistas o pérdidas de valor.
- Los costes por transacción son casi nulos.
- Se pueden comprar o vender BTC en mercados de intercambio de divisas, basadas en la reputación de cada usuario.

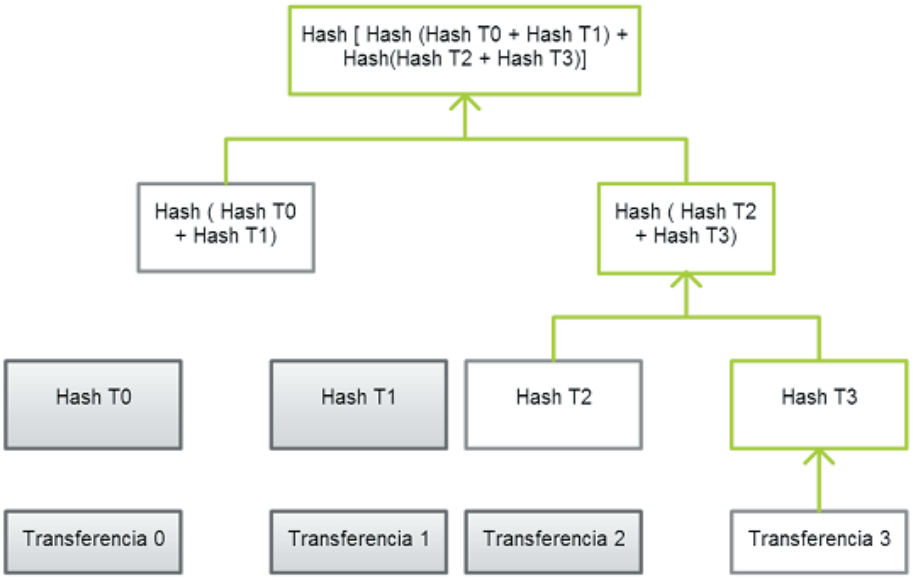

Figura 3. Árbol hash. Fuente: Wikimedia Commons.

> “La Autoridad de Servicios Financieros de Japón planea designar a la divisa virtual Bitcoin como una moneda corriente, con el fin de reforzar la protección de sus usuarios y facilitar su uso”

Los principales inconvenientes son los siguientes [9]:

- Financiación de actividades ilícitas y/o blanqueo de capitales. Debido al carácter descentralizado, la transmisión del valor monetario se produce directamente entre el ordenante y el beneficiario de la operación. Ésto dificulta la identificación y alerta temprana en actividades ilícitas.
- Efectos reputacionales negativos. El empleo generalizado de sistemas de pago electrónicos por parte de redes de crimen organizado deteriora la confianza del público.
- Tendencias oligopolísticas en la creación de la moneda virtual. La asignación asimétrica de unos recursos monetarios favorece a aquellos con mejores conocimientos técnicos y en recursos informáticos, frente a los mecanismos de mercado.
- Posibles transacciones fraudulentas. Desajustes en el ritmo de actualización de software de los distintos nodos de la red, han ocasionado puntualmente la aceptación de transacciones duplicadas. A posteriori rechazadas en otros puntos de validación.
- Impacto sobre la estabilidad de los precios. El uso de BTC’s podría llegar a afectar a la demanda de los pasivos de un banco central, impactando en el nivel general de precios de la economía y la efectividad de las medidas de política monetaria.
- Impacto sobre la estabilidad financiera. Las plataformas privadas de intercambio de BTC’s por monedas de curso legal, están marcadas por la elevada volatilidad de las cotizaciones debido a movimientos especulativos.
- No dispone de derecho de reembolso. Debido a su configuración, a modo de cadena de transacciones, el traspaso de bitcoins entre usuarios es firme e irreversible. Ésto impide poder disfrutar de un mecanismo de protección equivalente.

3.6. El futuro de Bitcoin

La Autoridad de Servicios Financieros de Japón ha promovido para 2016 [10] un nuevo marco legal para las entidades que ofrezcan servicios relacionados con divisas virtuales. Éstas deberán someterse a la supervisión de las autoridades japonesas y así prevenir nuevos casos como el escándalo en 2014 de Mt.Gox[3], a raíz del cual, Japón aprobó una normativa pionera para tipificar esta criptomoneda[4] como una mercancía y no como una divisa.

La Autoridad de Servicios Financieros planea designar a la divisa virtual Bitcoin como una moneda corriente, con el fin de reforzar la protección de sus usuarios y facilitar su uso. El cambio permitirá que el Bitcoin sea empleado como una forma de pago equivalente a otras unidades monetarias, además de que las divisas virtuales sean intercambiadas por monedas de curso legal sin control de ningún banco o autoridad monetaria.

El objetivo es responder a la creciente demanda de estas divisas, garantizar la protección de sus usuarios y facilitar el desarrollo del sector tecnológico, en especial las transacciones comerciales y financieras a través de Internet.

Nuevamente, Japón se sitúa a la vanguardia de la regulación de las divisas digitales, pues la nueva normativa será aprobada por la Dieta[5] durante la actual legislatura, según Nikkei.

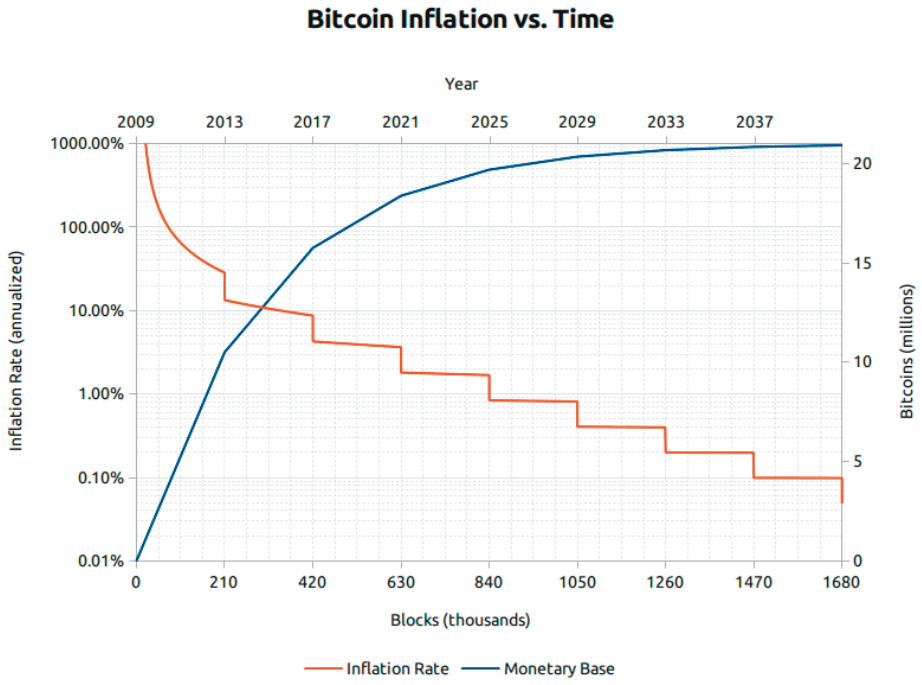

Figura 4. Gráfico sobre los bitcoins generados en el tiempo Fuente: Wikimedia Commons.

4. Otras monedas virtuales

El equipo jamaiquino [11] clasificado para las Olimpíadas de Invierno de Rusia en Sochi 2014 recaudó $25.000 en la moneda virtual Dogecoin en apenas unas pocas horas, con la finalidad de recaudar fondos para participar en el evento.

Conocer cuántos tipos de monedas virtuales existen en la actualidad es complicado. El portal web Coinmarketcap[6] registra la capitalización bursátil de una lista de 78 divisas en tiempo real. Entre ellas destacamos:

- **Litecoin**: En circulación desde el 2011. Ha llegado a cotizarse algunos días en 0,05$ y 48$. Utiliza el mismo sistema de Bitcoin, si bien la confirmación de las transacciones se produce con mayor rapidez (<3 minutos) y el proceso de *mining* puede realizarse con equipos de menor capacidad.
- **Peercoin**: Disponible desde 2012. Seguridad y eficiencia energética son parte de la oferta de esta divisa. Se denomina

"ecológica", pues la verificación de las transacciones por el método "*proof-of-stake*" (operaciones para probar que son los legítimos propietarios de la moneda) es más sencilla que la de Bitcoin "*proof-of-work*", que con algoritmos complejos hacen que la computadora trabaje excesivamente. Además, elimina el proceso colectivo de *mining*, identificado como un fallo en Bitcoin ya que su propósito es obtener ganancias, lo que va en contra de sus "principios democráticos".

- **Quark**: Creado en 2013, su buen desempeño llevó a esta divisa a aumentar su valor en 500%, en solo una semana. Su cualidad principal es la seguridad. Utiliza seis funciones *hash* diferentes para proteger la información frente a una sola que utiliza Bitcoin. Las transacciones son mucho más rápidas y los envíos de dinero dentro de la red Quark son gratuitos a diferencia de Bitcoin.

Referencias

[1] Taringa! *Deep Web (Niveles, y que contiene cada uno)*. <http://www.taringa.net/posts/offtopic/16047905/Deep-Web-Niveles-y-que-contiene-cada-uno.html>. Último acceso: 30 de marzo de 2017.

[2] Platzi. *Silk Road, su historia y colapso*. <https://youtu.be/bHmZmpSdSjQ>.

Último acceso: 30 de marzo de 2017.

[3] Wikipedia. *Silk Road*. <https://es.wikipedia.org/wiki/Silk_Road>. Último acceso: 30 de marzo de 2017.

[4] Banco de España. *Eurosistema. Entidades Dinero Electrónico*. <http://www.bde.es/bde/es/secciones/normativas/Regulacion_de_En/Estatal/Entidades__de_d_be3472d6c1fd821.html>. Último acceso: 30 de marzo de 2017.

[5] Andbank. *¿Qué son las entidades de dinero electrónico?* www.andbank.es/observatoriodelinversor/que-son-las-entidades-de-dinero-electronico/>. Último acceso: 30 de marzo de 2017.

[6] Javier Areitio Bertolín. Análisis de Bitcoin: Sistema P2P de pago digital descentralizado con moneda criptográfica virtual. *Novática nº222, marzo-abril 2013*, pp. 34-41. <http://www2.ati.es/novatica/2013/222/nv222sum.html>.

Último acceso: 30 de marzo de 2017.

[7] Finanzas para todos. *Bitcoin: origen, funcionalidades y riesgos de la moneda virtual.* <http://www.finanzasparatodos.es/es/secciones/actualidad/bitcoin.html>. Último acceso: 30 de marzo de 2017.

[8] Javier Hernando. *¿Qué es Bitcoin y por qué se habla tanto de ello últimamente?* United Explanations, Economía, 19/02/2013. Último acceso: 30 de marzo de 2017. <http://www.unitedexplanations.org/2013/02/19/que-es-bitcoin-y-por-que-se-habla-tanto-de-ello-ultimamente/>. Último acceso: 30 de marzo de 2017.

[9] Sergio Gorjón. *Divisas o Monedas Virtual: El caso de Bitcoin.* Banco de España EuroSistema, enero 2014. <http://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_Bitcoin_enero2014.pdf>. Último acceso: 30 de marzo de 2017.

[10] Agencia EFE. *Japón considerará al Bitcoin como divisa para fomentar su uso y su seguridad.* EFE Tokio, 24 febrero 2016. <http://www.efe.com/efe/america/economia/japon-considerara-al-bitcoin-como-divisa-para-fomentar-su-uso-y-seguridad/20000011-2848609>. Último acceso: 30 de marzo de 2017.

[11] BBC. *No solo Bitcoin: cuáles son las otras monedas digitales*. 22 enero 2014. <http://www.bbc.com/mundo/noticias/2014/01/140122_tecnologia_monedas_digitales>. Último acceso: 30 de marzo de 2017.

[12] El Mundo. *La compañía de intercambio de bitcoins Mt.Gox se declara en quiebra en Japón*. 28 febrero 2014. <http://www.elmundo.es/tecnologia/2014/02/28/53105fd3268e3eaf138b456d.html>. Último acceso: 30 de marzo de 2017.

Notas

[1] *Clearers*.

[2] *Peer-to-Peer*.

[3] La empresa Bitcoin Mt Gox se lanzó en marzo de 2011 por Karpeles y fue la compañía más grande en el mercado de Bitcoin en su momento, llegando a manejar alrededor del 70% de las transacciones en todo el mundo. En febrero de 2014, se declaró en quiebra y reveló la desaparición de una enorme cantidad de esta moneda virtual [12].

[4] Forma de pago que tiene en la encriptación de datos el respaldo de su valor material.

[5] Parlamento nipón.

[6] <http://coinmarketcap.com>.