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*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia<secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Padilla 66, 3º, dcha, 28006 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Lenguaje primario - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 222, marzo-abril 2013, año XXXIX

Tema del próximo número: "Minería de procesos"

Análisis de Bitcoin: Sistema P2P de pago digital descentralizado con moneda criptográfica virtual

Javier Areitio Bertolín
Catedrático de la Facultad de Ingeniería, Universidad de Deusto, Director del Grupo de Investigación Redes y Sistemas; Coordinador de la sección técnica "Seguridad" de Novática

<jareitio@deusto.es>

Resumen: *En el presente artículo se identifica y analiza Bitcoin desde la perspectiva técnica, bajo el punto de vista de su ciberseguridad. El* bitcoin *(o BTC) generado por GPUs (*Graphic Processing Units*), puede fragmentarse hasta 0,00000001 BTC, y está construido en deflación para evitar la inflación, de modo que nunca pueda haber más de 21 millones de BTC. Puede ser clasificado a la vez dentro de muchas categorías: sistema de dinero criptográfico virtual/ digital / electrónico con cierto grado de anonimato, P2P, software libre, descentralizado,* v-money/cyber-cash*,* virtual-cash*, etc. Su campo de aplicaciones va de los micropagos a los mercados de comercio del mundo virtual con costos de transacción bajos. Las transacciones y bloques son sus principales estructuras de datos y las monedas su bloque fundamental de construcción (cada moneda posee un identificador único, una cantidad de BTC y un propietario). No hay autoridad central y las transacciones las verifican las entidades semejantes. Se basa en redes P2P abiertas y criptografía asimétrica (firmas digitales bajo ECC 256 bits) y funciones* hash *(SHA-256/ RIPEMD160) para mantener su integridad. Las direcciones* bitcoin *son claves públicas y una moneda BTC es una cadena de firmas digitales, es decir, transacciones firmadas criptográficamente.*

Palabras clave: *Árbol Merkle,* bitcoins/BTCs*, bloques, ciberriesgos, ciberseguridad, firmas digitales ECDSA,* hash*,* malware*, moneda criptográfica virtual, PoW, sistema P2P de pago digital descentralizado, transacciones.*

1. Introducción

Se constata hoy en día una creciente volatilidad de la *economía* motivada por la introducción masiva de nuevas tecnologías, como por ejemplo los *programas bots* para la realización de operaciones automáticas a muy alta velocidad en el área de las Bolsas a nivel mundial.

Así mismo se observa un crecimiento vertiginoso en los últimos años de las *comunidades virtuales digitales* y de la *economía conducida a través de Internet.*

Este fenómeno se ha visto favorecido por los *medios sociales* y por el *cambiante mundo* en que vivimos. En este *entorno* donde van surgiendo nuevos *modelos de e-business* [1][2], *bitcoin* representa una opción de *dinero virtual digital* para el intercambio de bienes-servicios y efectuar donaciones [3][4].

El *sistema bitcoin* combina la *PoW* (*Proof-of-Work, encontrar el nonce*[1] *que permita calcular un hash de bloque que empiece con el número requerido de bits cero*) con una *cadena hash* lo que resuelve el problema de la *marca de tiempo distribuida* de cara a prevenir el *problema del doble gasto.* Los costos de las transacciones son mucho más bajos [5][6] y la creación de dinero y las transacciones las gestiona colectivamente una *red abierta P2P.*

Fue inventado en el *2008* por *Satoshi Nakamoto* (*posiblemente sea un pseudónimo*) [4], si bien la idea pionera referente al *dinero digital* data de *1982* con el desarrollo *e-cash* de *David Chaum.*

Bitcoin puede considerarse bajo tres prismas:
1) Como una *moneda virtual* o forma innovadora de establecer *dinero digital* a través de *Internet.* Se trata de un sistema de pago *open-source*, basado en red P2P abierta, descentralizado, que utiliza transacciones irrevocables y fundamentado en PoW.
2) Como un nuevo tipo de *sistema de pago* o *medio de intercambio / moneda/BTC / dinero electrónico 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 *bitcoins*, ni de *tercera parte de confianza* o *TTP* para posibilitar o supervisar las *transacciones online.*
3) Como un *protocolo criptográfico* para procesos financieros en nuevos modelos de *e-business* y *e-commerce*, donde se observa un crecimiento importante en el área de la *criptografía financiera* [7][8]. La consultora *Juniper Rearch* estima que el desarrollo del *e-commerce* supondrá que el mercado de los pagos móviles alcance este mismo año los *seiscientos mil millones de dólares* en todo el mundo.

2. Modos de utilización

Para utilizar Bitcoin *se debe* instalar un cliente de software libre *en computadores (*bitcoin-qt, armony, bitcoinspinner, etc.*) o ejecutar una* aplicación móvil *sobre* smartphones/ dispositivos móviles *(*coinbase, bitcoin-wallet, etc.*) que genera direcciones* [9].

Se pueden identificar tres modalidades de monederos que contienen entre otras cosas pares de claves para cada dirección, transacciones desde o hacia tus direcciones y las preferencias del usuario:
a) *Monederos sobre PCs/Macs*. Se instalan sobre un computador. Proporcionan control total de su monedero, y exigen hacer copias de seguridad y proteger el dinero.
b) *Monederos móviles*. Permiten tener *bitcoins* en el bolsillo, se puede pagar o intercambiar monedas escaneando un *código óptico QR* o utilizando *tecnología RF NFC* por ejemplo a través de un *smartphone* o *smartcard.*
c) *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 bitcoin* en un sitio web.

Existen diversos tipos de clientes *bitcoin*, por ejemplo los de minería sólo pueden realizar minería, los de sólo firma sólo pueden firmar transacciones, los completos pueden firmar transacciones, generar cabeceras de bloque y cadenas de bloques pero no pueden realizar minería, y los ligeros no pueden realizar ni minería, ni firmar transacciones, ni cabeceras de bloque ni cadenas de bloques.

3. *Utilidad de los* Bitcoins

La creación del *sistema bitcoin* responde entre otras a las siguientes razones:
1) Las transacciones realizadas utilizando enfoques convencionales de pago electrónico presentan elevadas tasas.
2) Actualmente se detecta un incremento de las tecnologías digitales descentralizadas como *multi-Torrent.*
3) *Paypal* y otros sistemas afines pueden actuar como sistemas de vigilancia lo que vulnera la privacidad de las personas que los utilizan.

En la actualidad *Bitcoin* ha dejado de ser sólo un experimento-proyecto y se ha convertido también en una realidad ya que se constata que va creciendo el número de sitios donde se acepta y puede utilizarse:
a) ***Negocios que aceptan bitcoin***[2]. Numerosos comercios permiten el pago a través de *bitcoins*: <bitcoinstore.com> (*produc-*

> *Bitcoin* se basa en firmas digitales para probar la propiedad y de una historia de transacciones pública para prevenir el doble gasto

tos electrónicos), <pirateofsavannahbook.com> (libros), <gemsofasia.com> (ropa, bolsos, etc.), <videoseconds.com> (*películas, DVD/CDs*, etc.), <siglotienda.com>, etc. También plataformas de *e-commerce* como wordpress.com store, drupal.com, zencart.com, prestashop. com, oscommerce, magento, woocommerce, etc.

El sistema *bitcoin* ya opera en *servicios online* de hospedaje web, teléfono por Internet, desarrolladores web, etc. Como por ejemplo: *Sandalo, V-Storage, Pharmacy, We-design, Online-mobile-Stores*, etc. [10][11].

b) ***Entidades que aceptan o han aceptado donaciones***: *EFF (Electronic Frontier Foundation), aunque no actualmente, FSF* (*Free Software Foundation*), *XKCD* (*Webcomic*), *Wikileaks,* entidades de recepción de donaciones de caridad, etc.

Bitcoin es una *moneda criptográfica* (*o forma de pago alternativa a PayPal, tarjetas electrónicas*) para comunicar por correo electrónico [12], por mensajería instantánea, etc. que las *webs* publican y las *Redes Sociales* socializan.

Las *principales formas de obtener BTCs* son:
1) Cambiando una moneda como el euro, dólar, etc. a *BTCs. Mt. Gox* es uno de los mayores *centros de intercambio*[3].
2) Vendiendo-subastando algo.
3) Generándolo, actuando como *minero* del *sistema bitcoin.*

Bitcoin es *dinero criptográfico virtual descentralizado* que utiliza *primitivas cripto-gráficas* y *minería* (es decir "*resolución de puzzles*" o *PoW* difíciles) para verificar transacciones, prevenir el doble gasto, recoger tasas de transacción, proporcionar transacciones irrevocables y protegerse contra la inflación.

Se basa en *firmas digitales* para probar la propiedad y de una *historia de transac-ciones* pública para prevenir el doble gasto. La historia de las transacciones se comparte utilizando una *red P2P abierta* y se acuerda utilizando un sistema de *prueba de trabajo.*

Las primeras transacciones con *bitcoins* datan de enero del 2009, mientras que en junio de 2011 había 6,5 millones de *bitcoins* en circulación entre un colectivo estimado de diez mil usuarios y en *enero del 2013* el número de usuarios era de *cien mil* con una capitalización de mercado en torno a unos doscientos millones de dólares con unos once millones de *bitcoins* creados en circulación.

4. Diferencias entre dinero electrónico y dinero virtual. Bitcoins físicos

El *dinero virtual* como *bitcoin* puede considerarse un tipo específico de *dinero electrónico* utilizado para transacciones en el mundo *online* (*ciberespacio*) a través de Internet. El *ECB* (*European Central Bank*) establece diversas similitudes y diferencias entre el dinero electrónico y el dinero virtual:
1) En cuanto al ***formato del dinero***, el *dinero electrónico* y el *dinero virtual* ambos son *digitales.*
2) En lo relativo a la ***supervisión***, el *dinero electrónico* sí lo tiene, mientras que el *dinero virtual* no.
3) En lo referente a ***los tipos de riesgos***, el *dinero electrónico* presenta principalmente riesgos operacionales mientras que el *dinero virtual* los riesgos son legales, de crédito, de liquidez y operacionales.
4) En cuanto al ***estatus legal***, el *dinero electrónico* está regulado, mientras que el *dinero virtual* no lo está.
5) En lo relativo a la ***unidad de cuenta***, el *dinero electrónico* es dinero tradicional (euros, dólares, libras, etc.) con estatus de moneda de curso legal, mientras que el *dinero virtual* es dinero criptográfico inventado (por ejemplo, *bitcoins*) sin estatus de moneda de curso legal.
6) En lo referente a ***la aceptación***, el *dinero electrónico* es por compromiso del expendedor, mientras que el *dinero virtual* normalmente se utiliza dentro de una comunidad virtual específica.
7) En cuanto al ***expendedor***, el *dinero electrónico* lo establece legalmente una institución de dinero electrónico (por ejemplo *VISA MasterCard*), mientras que el *dinero virtual* como *bitcoin* surge a través de estructuras descentralizadas abiertas, de software libre, no financieras.
8) En lo referente a la ***posibilidad de canjear fondos***, en el *dinero electrónico* está garantizado (por valor), mientras que en el *dinero virtual* no está garantizado.
9) En lo relativo al ***suministro***, en el *dinero electrónico* está fijado, mientras que en el *dinero virtual* no lo está, depende de las decisiones del expendedor.

El *dinero* se intercambia en las transacciones en relación a compras de bienes y servicios. El dinero facilita el comercio de un bien por otro. Un buen dinero debe ser transportable, divisible (*fracciones de bitcoins se denominan satoshis*), corriente, escaso (*tendiendo a una cota máxima no alcanzable de 21 millones de bitcoins sólo podrán existir*) 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, diamantes, uranio, etc.), *digital centralizado* (*PayPal, WebMoney, e-gold, etc.*) o *digital descentralizado* que sostiene valor de intercambio sólo vía transacción electrónica (por ejemplo bitcoin).

Presenta *propiedades* como:
1) Unidad de cuenta. Valor definido; en *bitcoin* quizás con alta variabilidad.
2) Medio de intercambio. Aceptabilidad.
3) Almacén de valor. No perecedero.
4) Difícil de falsificar.
5) Debe permitir transacciones rápidas.
6) Debe prevenir el doble gasto. Se ha constatado la posibilidad de que surjan ataques del doble gasto en ciertas transacciones rápidas con *bitcoin.*
7) Con cierto grado de anonimato, *bitcoin* permite parcialmente el anonimato. El anonimato robusto no fue un objetivo de diseño del *sistema bitcoin.*

El *ciberespacio* se considera el quinto posible campo de batalla de cara a posibles incidentes, confrontaciones y *ciberataques* después de tierra, mar, aire y espacio/satélites.

Los *bitcoins* del mundo virtual, transferidos a través del ciberespacio ya se pueden sostener físicamente en forma de *tarjeta en el mundo real.* Por ejemplo, en <http://bitbills.-com> se crean *bitcoins físicos.* Se genera un par de claves criptográficas que se imprime sobre una tarjeta, donde se oculta la clave privada, en el exterior se incluye un *código óptico BIDI* QR y el valor en *bitcoins.* Para gastar de forma *online* los *bitcoins*, se escanea el código QR de la tarjeta.

5. Arquitectura de un sistema Bitcoin

Básicamente un *sistema bitcoin* incluye los siguientes *elementos*:
1) ***Una estructura de transacciones***. Permite especificar y cambiar la propiedad de los *bitcoins* (ver **figura 1**).

El bloque de construcción fundamental de *bitcoin* es la *moneda* que se caracteriza por un

> “El dinero virtual como *bitcoin* puede considerarse un tipo específico de dinero electrónico utilizado para transacciones en el mundo *online* (ciberespacio) a través de Internet. El ECB establece diversas similitudes y diferencias entre el dinero electrónico y el dinero virtual”

identificador único y una cantidad (o denominación), es decir un número arbitrario y un propietario.

Las monedas pueden dividirse y juntarse. Si una entidad A desea enviar *bitcoins* a otra entidad B unirá algunas de sus monedas y dividirá el resultado entre A y B.

El propietario de una moneda se identifica por una dirección, cada *dirección* esta asociada con una *clave privada*. Para utilizar una moneda el propietario debe proporcionar una *firma digital* con la clave privada asociada utilizando el *algoritmo criptográfico ECDSA (ver* **figura 2***)*.

El proceso donde las monedas se juntan y dividen se denomina *transacción*, se utiliza para mover *bitcoins* de un propietario a otro.

Una *transacción* [13] puede tener cualquier número de entradas y salidas. Una salida especifica una dirección y una cantidad que se recibe. Una entrada referencia una salida previa no gastada. El valor total de todas las entradas debe ser al menos el valor total de todas las salidas.

La transacción se identifica por medio de un *hash* de sus datos. El *hash* debe firmarse con la *clave privada* correspondiente a cada dirección de entrada. Una *dirección* es un *hash* de una *clave pública ECDSA*. Una salida especifica un *script* con las condiciones para permitir gastarlo.

Si se utiliza la misma salida (o *moneda*) para pagar a dos receptores diferentes esto representa el *problema del doble gasto* (no existe acuerdo sobre quien es el verdadero receptor; debe existir alguna forma de determinar el orden de las transacciones). La solución que utiliza el *protocolo bitcoin* se denomina *cadena de bloques* (ver **figura 3**).

Las transacciones se agrupan en bloques, los bloques se confirman utilizando una *PoW* (*prueba de trabajo*). Una transacción se considera final si se incluye en un bloque confirmado.

Cada bloque referencia un bloque previo para formar una cadena. En caso de conflicto, gana la transacción con más gasto de potencia de computación en confirmación. Los ataques necesitan tener más potencia de computación que el resto de la *red abierta P2P*[4].

2) ***Una red abierta P2P***
Posibilita propagar, verificar y almacenar los datos de la transacción.

Las nuevas transacciones se difunden a todos los nodos; cada nodo recoge nuevas transacciones en un bloque. Cada nodo opera encontrando un *PoW* difícil para su bloque. Cuando un nodo encuentra un *PoW* difunde el bloque a todos los nodos.

Los nodos sólo aceptan si todas las transacciones no se han gastado ya. Los nodos expresan su aceptación del bloque trabajando en crear el siguiente bloque de la cadena, utilizando el *hash del bloque* aceptado como *hash* previo.

La primera transacción de un bloque crea una moneda nueva. Es posible considerar dos tipos de estructuras en una *red bitcoin*:

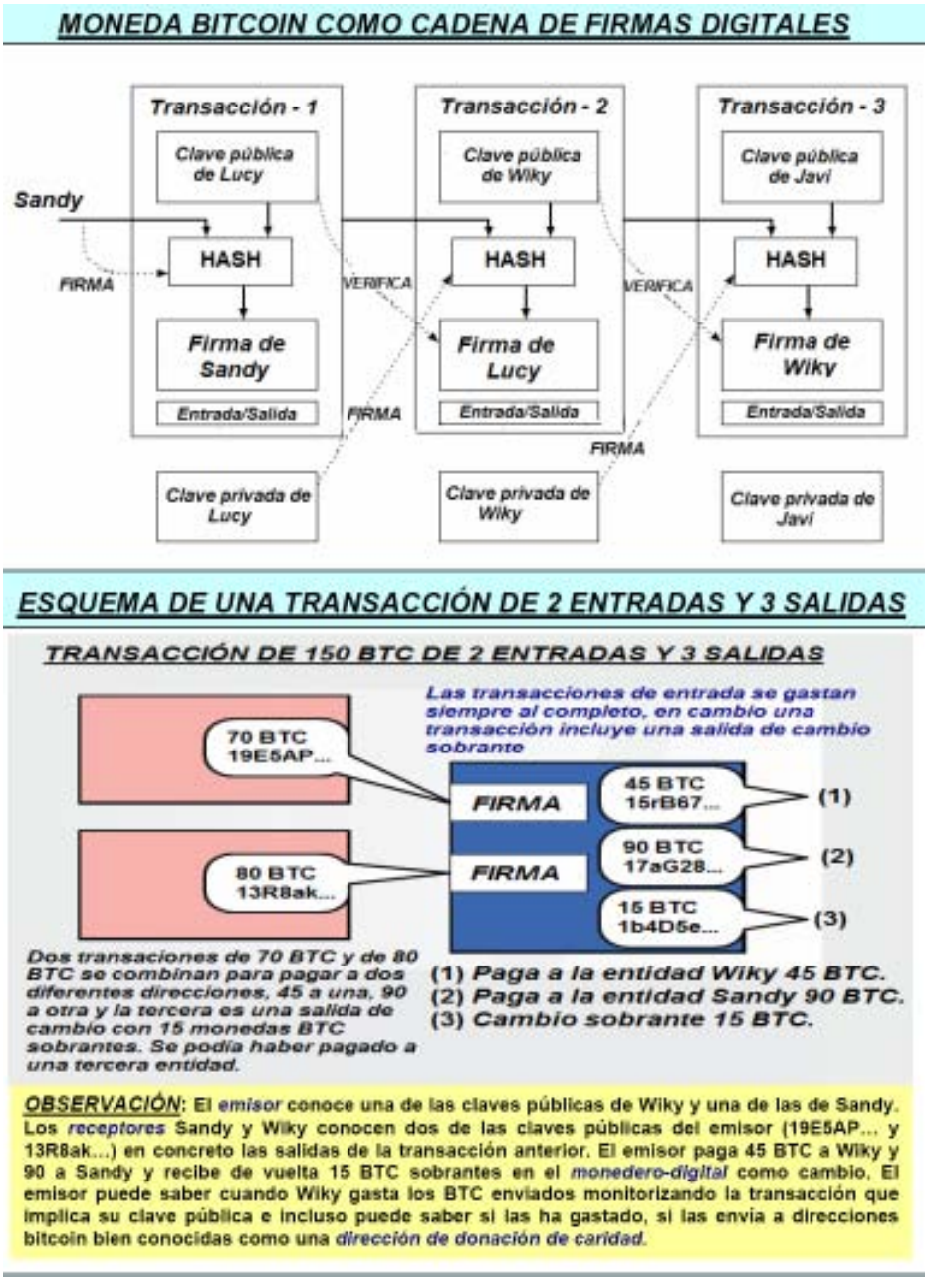


Figura 1. Estructura de transacciones en el sistema *bitcoin*.

EJEMPLO SIMPLIFICADO DEL ECDSA (ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM) UTILIZADO EN EL SISTEMA BITCOIN

(1) PROCESO DE GENERACIÓN DE LA FIRMA DIGITAL ECC:

(i) Sea m el mensaje a firmar digitalmente con la *clave privada* de la entidad firmante. Se selecciona una curva elíptica sobre *GF(p)*, por ejemplo: $y^2 = (x^3 + 7.x + 9) \ mod \ 11$ definida sobre GF(11). Se selecciona un punto G de ella cuyo orden n sea el número de puntos de la curva. Aquí la curva tiene 17 puntos. En este caso, elegimos como punto G = (5,9) que cumple *17.G = O*. Por tanto n = 17.

(ii) Sea d la *clave privada* del firmante y Q la *clave pública* del firmante. En este caso si la clave privada d = 11 entonces: Q = d.G = 11.(5, 9) = (7, 4).

(iii) Se calcula e = *HASH(m)* donde la función criptográfica unidireccional *HASH* puede ser: *SHA-1, SHA-512, MD5, RIPE*, etc. Por ejemplo e = *HASH(m)* = 17.

(iv) Se selecciona un número entero aleatorio k dentro del intervalo [1, n – 1] por ejemplo: k = 9. Se calcula: *k.G = (x1, y1)* y se determina: *r = x1 mod n*. Si *r = 0* entonces se vuelve al punto (iv). En este caso k.G = 9.(5, 9) = (10, 10) = (x1, y1) se calcula: r = x1 mod 17 = 10 que es distinto de cero.

(v) Se calcula: $s = k^{-1}.(e + d.r) \ mod \ n$. Si el resultado *s = 0* se vuelve al punto (iv). En este caso: $s = 9^{-1}.(17 + 11.10) \ mod \ 17 = 2.(127) \ mod \ 17 = 254 = 16$. Como s es distinto de cero, es un valor válido. Por tanto, la *firma digital ECDSA* obtenida es el par de valores enteros: *(r, s) = (10, 16)*.

(2) PROCESO DE VERIFICACIÓN DE LA FIRMA DIGITAL ECC:

(i) Para que el receptor pueda autenticar la firma (r, s) recibida junto al mensaje m del *emisor o firmante* necesita saber la *clave pública del firmante Q*. En este caso: (r, s) = (10, 16) y Q = (7, 4).

(ii) Se verifica que r y s sean números enteros en el intervalo [1, n – 1]. En caso contrario la firma digital no es válida. En este caso es válida.

(iii) Se calcula: *e = HASH(m)*. En este caso: e = 17. Se obtiene: $w = s^{-1} mod \ n$. En este caso: w = 16. Se determinan los valores: *u1 = e.w mod n* y *u2 = r.w mod n*. En este caso: u1 = 17.16 = 0, u2 = 10.16 = 7. Se halla: *u1.G + u2.Q = (x1, y1)*. En este caso: 0.(5, 9) + 7.(7, 4) = (10, 10) donde x1 = 10.

(iv) La *firma es válida* si se cumple que: *x1 = r mod n*. En este caso: 10 = 10 mod 17 → Por tanto *la firma se ha verificado que es válida.*

Figura 2. Algoritmo de firma digital ECDSA usado en *Bitcoin*.

a) ***Red de transacciones***. Representa el *flujo de bitcoins* entre transacciones a lo largo del tiempo.
b) ***Red de usuario***. Representa el *flujo de bitcoins* entre los usuarios a lo largo del tiempo.
3) ***Un sistema PoW*** (*de prueba de trabajo*) (*hashing, "minería"*).

Permite sincronizar las transacciones y determinar la distribución inicial de las monedas criptográficas [4].

5. Mecánica operativa de Bitcoin. Operaciones de minería

Las organizaciones (*empresas, comercios, negocios, etc.*) se mueven cada vez con más presencia en el ciberespacio (o *espacio virtual*) y se mueven en ese territorio porque los usuarios, consumidores, proveedores, socios corporativos, etc. ya se encuentran allí. *Bitcoin* es un *sistema de pago P2P descentralizado* que se basa en *PoW* [14]. Los pagos se realizan generando transacciones que transfieren monedas denominadas *bitcoins* (*o abreviadamente BTCs*) entre *usuarios de bitcoin.*

Los usuarios participan en las transacciones utilizando pseudónimos denominados *direcciones bitcoin.* Normalmente cada usuario tiene cientos de *direcciones bitcoin* diferentes que se almacenan y se gestionan en su *monedero digital.* Cada dirección se hace corresponder por medio de una función de transformación a un único par de *claves criptográficas pública-privada.*

Estas claves se utilizan para autorizar la transferencia de la propiedad de los *bitcoins* entre direcciones. Los usuarios se transfieren entre si las *monedas bitcoins* emitiendo una transacción [9].

Una transacción se forma firmando digitalmente un *hash de la transacción* a través de la que se adquirió un *bitcoin.*

Dado que en el *sistema bitcoin* existe una correspondencia uno a uno entre las claves públicas de firma y las direcciones, *una transacción* que tiene lugar entre dos direcciones *d1* y *d2* tiene la forma *T = (origen, k, d2, F(origen, k, d2))* donde F representa la firma utilizando la clave privada que corresponde a la clave pública asociada con *d1*. El valor *k* representa la *cantidad de bitcoins* transferidos y el *origen* es una referencia a la transacción más reciente desde la que *d1* adquirió los k *bitcoins.*

Después de su creación, las *transacciones bitcoin* son liberadas a través de la *red abierta P2P bitcoin.* Una vez se confirma la validez de la transacción *T, d2* puede utilizar esta transacción como una referencia para gastar los *bitcoins* adquiridos.

Consecuentemente las *transacciones con bitcoin* forman un *registro público* y cualquier usuario puede verificar la autenticidad de un *bitcoin* comprobando la *cadena de firmas digitales* de la transacción en la que estuvo implicada el *bitcoin.*

En el caso en que d1 necesite gastar un valor que exceda al valor máximo de *bitcoins* que posea, entonces *su cliente bitcoin* automáticamente combina un conjunto de *bitcoins* como múltiples entradas de la misma transacción de salida, dando lugar a una *transacción multi-entrada.*

En la actual implementación de *bitcoin*, automáticamente se crea y utiliza una nueva dirección (denominada *shadow-address*) para recoger el *cambio* que resulta de cualquier transacción emitida por el usuario. Además de la dependencia en pseudónimos, las *shadow-address* constituyen el único mecanismo adoptado por *bitcoin* para proteger la *privacidad de sus usuarios.*

Las transacciones se difunden a través de la *red abierta P2P bitcoin* y son sujeto de comprobaciones de validez por parte de los usua-

> Cuando un *minero* genera un bloque con éxito se le concede como recompensa un cierto número de nuevos bitcoins. Esto proporciona un incentivo para los mineros lo que permite soportar de forma continua el sistema *bitcoin*

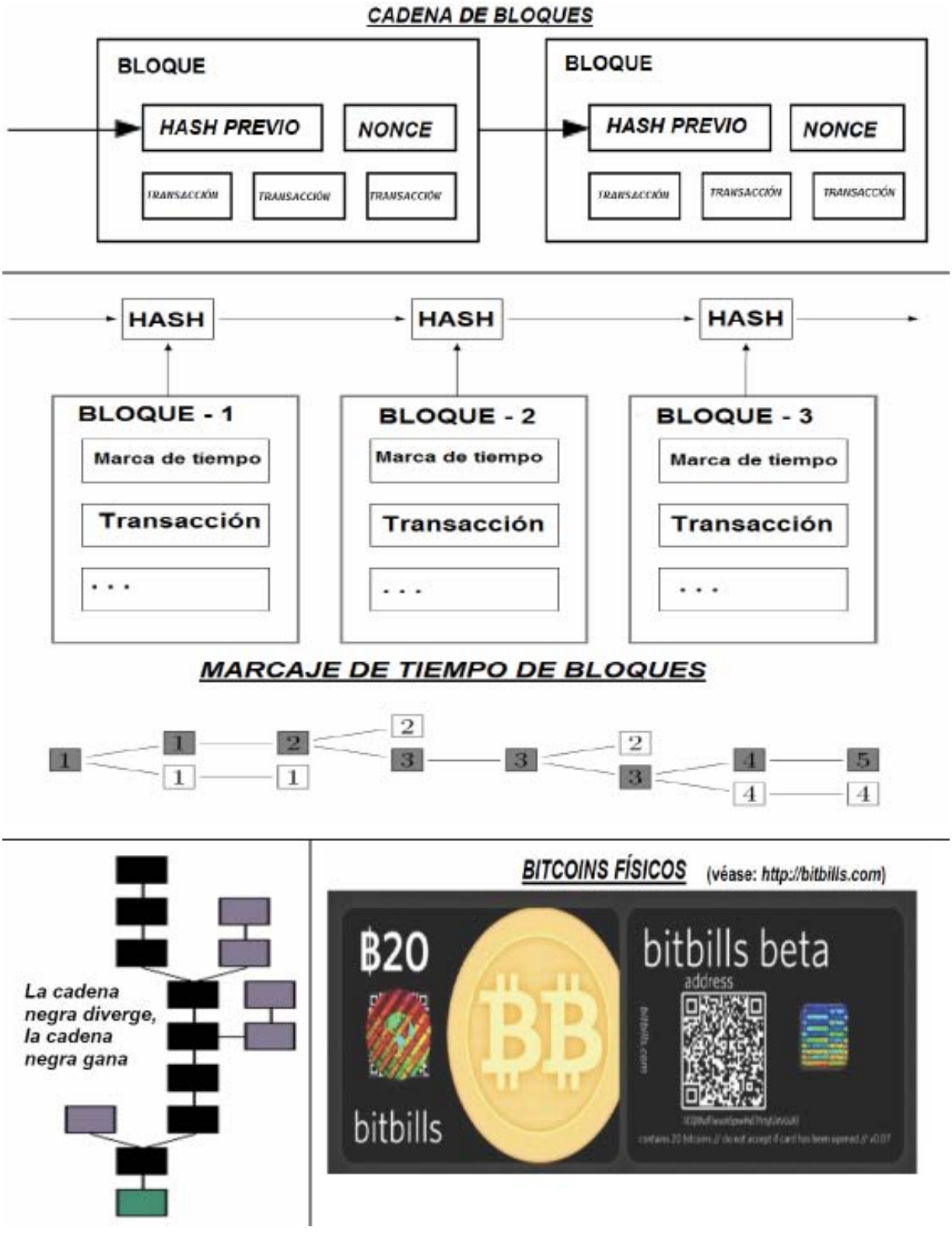
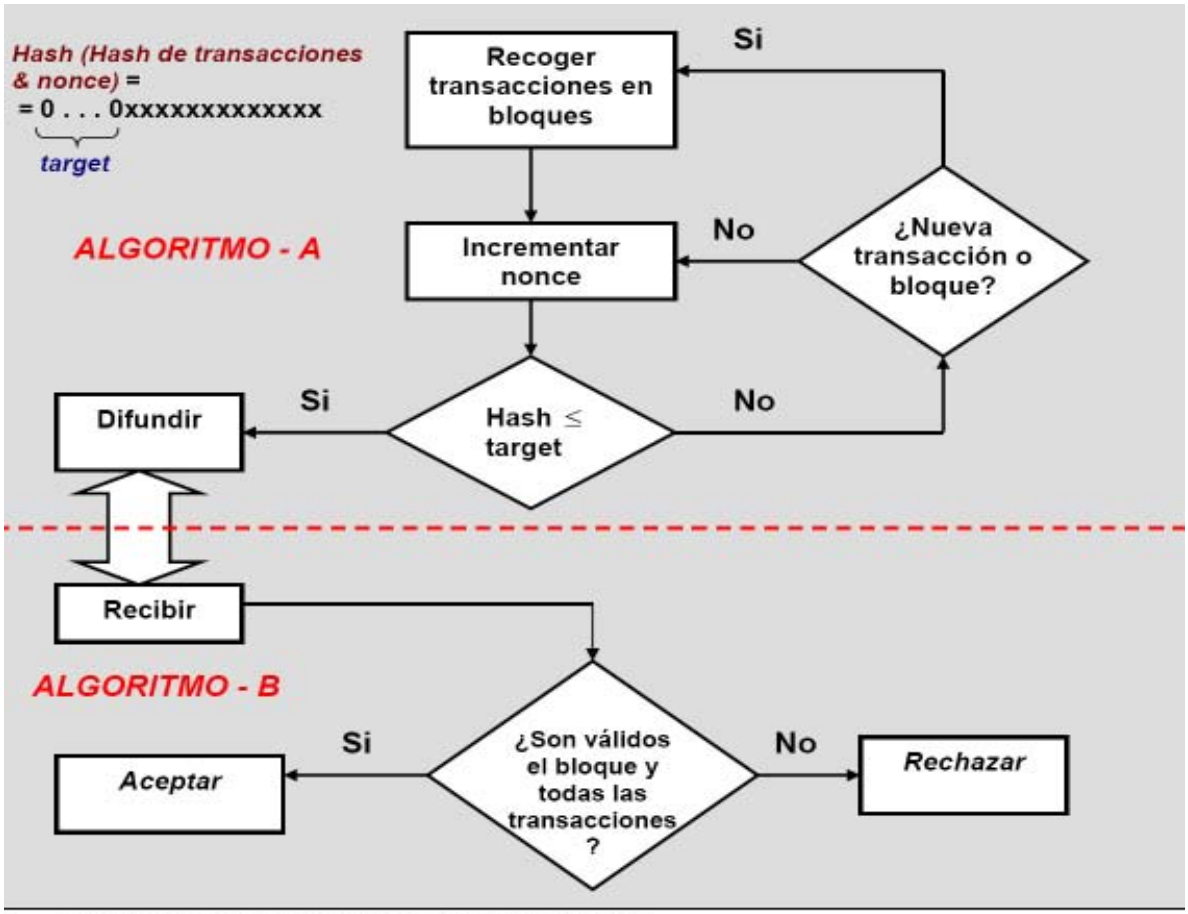


Figura 3. Cadena de bloques en *Bitcoin*.



- Cada nodo recoge nuevas transacciones en un bloque.
- Las transacciones se aceptan si su bloque está validado.
- La cadena contiene todas las transacciones hechas por la red.
- Cada nodo tiene una copia completa de la creciente cadena de bloques.
- Para validar un bloque cada nodo trabaja para resolver un PoW difícil.
- El *PoW* consiste en encontrar el *nonce* que permite calcular un *hash de bloque* que empieza con el número requerido de bits cero. Usar potencia de CPU para calcular el nonce correcto.
- El primer nodo que encuentra el PoW envía el bloque al resto de la red P2P.
- Si el bloque se acepta, el nodo comienza construyendo el siguiente bloque de la cadena, en caso contrario, el nodo continúa trabajando con la cadena más larga.
- Si varios bloques llegan simultáneamente (dos versiones de cadena de bloques) sólo se selecciona la más larga.
- Todos los nodos que generan (o *mineros bitcoin*) ejecutan el *algoritmo A* tratando de encontrar *un hash* de bloque menor corriente hash destino.
- Esto sirve para dos objetivos: (i) limitar el número de bitcoins creados con el tiempo. (ii) Es una forma equitativa de seleccionar que transacciones se considerarán válidas.
- Todos los nodos de la red P2P comprueban su trabajo (*algoritmo B*) y no aceptarán bloques inválidos.
- El incentivo para mineros bitcoin es encontrar bloques, primero transacciones en cada bloque crean nuevos bitcoins, los mineros crean una transacción que les paga nuevas monedas sacadas de la mina.
- Los *BTCs* (*Bitcoins*) son realmente transacciones firmadas criptográficamente.

Figura 4. Mecánica del POW en el sistema *Bitcoin.*

rios del sistema. Las transacciones válidas las incluye un tipo especial de usuarios denominado *mineros* en bloques *bitcoins* que también son difundidos en la red.

Para generar un nuevo bloque, los *mineros* deben encontrar un valor *nonce* que cuando se haga *hash* con campos adicionales (*el hash de Merkle de todas las transacciones válidas recibidas*, *el hash del bloque previo y una marca de tiempo*) resulte en un valor por debajo de un umbral dado. Si se encuentra tal *nonce*, los mineros lo incluyen en un bloque de modo que se permita a cualquier entidad verificar la *PoW*.

Cuando un *minero* genera un bloque con éxito se le concede como recompensa un cierto número de nuevos *bitcoins*. Esto proporciona un incentivo para los mineros lo que permite soportar de forma continua el sistema *bitcoin*. El bloque resultante se reenvía a todos los usuarios de la red que pueden comprobar su corrección verificando el cálculo del *hash*. Si el bloque se considera válido entonces los usuarios lo añaden a sus bloques previamente aceptados, de modo que crece la *cadena de bloques bitcoin* (ver figura 4).

Bitcoin se basa en este mecanismo para resistir a *ataques de doble gasto*. Los usuarios maliciosos que deseen realizar el *doble gasto* de *bitcoins* sin ser detectados deberían no sólo rehacer todo el trabajo para calcular el bloque donde se gastó esos *bitcoins* sino también recalcular todos los bloques subsiguientes de la cadena. La tasa de generación de bloques es de seis bloques cada hora como la cabecera

> “Los fallos del sistema o los errores humanos pueden causar la pérdida accidental del fichero monedero que guarda las claves privadas necesarias para gastar las monedas”

de cada bloque ocupa ochenta bytes entonces al año se generan 4,2 Mbytes de cabeceras.

6. Cuestiones de ciberseguridad en sistemas *Bitcoin*

Se han podido constatar e identificar diversos tipos de *ciberriesgos* y *ciberincidentes* desde su aparición:

1) *Robo o pérdida de bitcoins.* Lo que permite a un usuario gastar *monedas BTCs* es la posesión de la *clave privada* asociada. Todos los *bitcoins* son de conocimiento público en forma de salidas de transacción no amortizadas. Consecuentemente el robo o la pérdida de claves privadas o la falsificación de firmas digitales dan lugar a la pérdida de dinero. Por ejemplo, en marzo del 2012, se robaron *43.000 bitcoins* de la plataforma de comercio *Bitcoinica.* En junio del 2011, se produjo un robo de medio millón de dólares en *bitcoins*[5] .

2) *Acceso no autorizado y modificaciones en la base de datos de bitcoin.* El atacante modifica el número de *bitcoins* disponibles en el mercado añadiendo dos millones de *bitcoins* falsos[6] .

3) *Ataques con código malicioso o malware.* Los dispositivos de computación de usuario (*PCs, Macs, smartphones, tablets, etc.*) pueden ser infectados con *malware* o incluir *clientes falsificados.* El servicio de *monedero online mybitcoin.com* ha perdido recientemente por malware 1,3 millones de dólares de monedas de usuario vía malware[7] .

Algunas de las *ciber-contramedidas* posibles son:

a) Herramientas multi-funcionales de ciberseguridad [15] con *antimalware, firewall, IDS-IPS, DLP,* etc.

b) *Monedero maestro-secundario.* Se trata de un pequeño *banco personal* de usuario donde se almacenen la mayor parte de sus monedas. El *monedero-maestro* se divide a través de varios dispositivos de compu-tación utilizando técnicas basadas en tecnología umbral. El usuario lleva un pequeño *monedero-secundario* en su *smartphone.* Se establecen transacciones preaprobadas para que el usuario pueda sacar dinero de su *monedero-maestro* a su *monedero-secundario* de forma periódica en pequeñas cantidades de forma similar a cómo los bancos reales permiten sacar dinero a sus clientes desde sus *cajeros automáticos.*

c) *Criptografía umbral.* Consiste en dividir las *claves privadas* en varios fragmentos aleatorios utilizando técnicas de criptografía umbral y distribuirlas en diversas localizaciones, por ejemplo su PC, su *smartphone* y en un proveedor de servicios *online.* De esta forma sólo cuando se combine un número determinado de estos dispositivos el usuario podrá gastar sus monedas. Este enfoque penaliza la usabilidad a favor de la ciberseguridad.

4) *Pérdida accidental de BTCs.* Los fallos del sistema o los errores humanos fortuitos o provocados pueden causar la pérdida accidental del *fichero monedero* que guarda las *claves privadas* necesarias para gastar las monedas. Por ejemplo *bitomat* ha perdido recientemente doscientos mil dólares[8] motivado por la pérdida del fichero de claves privadas del monedero debido a haberlo hospedado en un almacenamiento de nube no persistente.

Como posibles cibercontramedidas:

a) Backups. Que se complican debido a que en *bitcoin* existe una creación incesante de claves.

b) Creación de las claves privadas a partir de una clave maestra o semilla utilizando un generador de números pseudo-aleatorios, esto reduce el backup a guardar una clave maestra o semilla en un sitio seguro.

c) Cifrado del monedero utilizando una contraseña robusta o múltiples contraseñas sencillas.

d) Esteganografía sobre el monedero.

e) Utilización de *hardware TP (Trusted-Path)* que permite introducir y leer datos ante posibles amenazas como el *malware.*

5) *Problemas de escalabilidad. Bitcoin* se basa en la difusión a tiempo de transacciones y bloques. Los adversarios podrían causar fallos en las comunicaciones utilizando herramientas automatizadas del tipo ataques *DoS/DDoS.* La celeridad excesiva de las transacciones-pagos podría generar ciertas vulnerabilidades en el *sistema bitcoin.*

6) *Problemas de privacidad.* La *comunidad bitcoin* es consciente de que el anonimato fuerte no fue uno de sus *objetivos de diseño*, consecuentemente podría ser posible correlacionar usuarios a sus claves públicas a partir de la historia completa de *transacciones bitcoin.*

Se ha constatado que cuando se incluyen una o más entidades intermedias (*para convertir dinero, monederos online, servicios de mixing, etc.*) en las transacciones con *bitcoins* se aumentan significativamente los riesgos de ciberseguridad.

La *comunidad bitcoin* reconoce ciertas debilidades en privacidad, la recomendación más común de utilizar servicios de mediación que intercambien *bitcoins* de diferentes usuarios presenta diversas limitaciones y ciberriesgos favoreciendo que los operadores puedan robar fondos, el seguimiento de monedas, etc.

Un usuario de *bitcoin* puede tener múltiples claves públicas, se considera una buena práctica de cara a la ciberseguridad generar un nuevo par de claves criptográficas pública-privada en cada transacción.

7) Otros problemas de *ciberseguridad*:

a) *Monedero guardado no cifrado.* Es el caso en el que un *código malicioso o malware* recupera el fichero *wallet.data* y lo envíe a un atacante. Esto supone que el atacante captura los pares de claves y puede *firmar* las transacciones en nombre del usuario. Una posible contramedida es cifrar el monedero.

b) *Rellenar la red con nodos infectados/maliciosos.* Es el caso de conectar cientos de miles de direcciones IP al *canal bootstrap IRC.* Esto supone conectarse sólo al canal del atacante que puede rechazar retransmitir tus bloques o tus transacciones dando lugar a posibles ataques de doble gasto. Una posible contramedida es limitar el número de direcciones IP que es posible conectar a un *canal IRC.*

c) *Conectar identidades a direcciones.* Es posible monitorizar si una *dirección bitcoin* se utilizó para firmar. Esto supone un seguimiento de la historia de la moneda y la pérdida del anonimato. Como posible contramedida emplear los servicios *eWallet* y no dejar información personal.

d) *Fallos del hardware.* Como contramedida realizar backups del monedero o su reinstalación.

e) *Movilidad de pagos.* En estos casos ambos lados de la transacción necesitan conexión a Internet, la cual quizás no este disponible.

f) *Ataques de criptoanálisis y side-channel a la implementación y gestión de claves.*

7. Consideraciones finales

El ***sistema bitcoin*** ya está aquí con todos nosotros [16] en medio de ***diversas consideraciones*** que hemos ido citando a lo largo del artículo, tales como: es software libre, no necesita control por parte de terceras partes ni autoridades centrales, no existe un único punto de fallo, permite aplicaciones avanzadas, reducidos costos de transacción online, permite compra online pseudo-anónima (*manteniendo las claves*

> "Las transacciones *bitcoin* que se pueden observar actualmente son relativamente simples (por ejemplo, pagar con una clave pública una cantidad de bitcoins), pero en el futuro cabe pensar en transacciones más complejas"

públicas pseudo-anónimas), los atacantes necesitan tener más potencia de computación que el resto de la *red abierta P2P*, necesidades bajas de infraes-tructura, es internacional, carencia de banca legal, cuestiones legales pendientes no resueltas, su valoración fluctúa [17] (*algunos comerciantes que venden productos físicos se quejan de la elevada volatilidad del precio hora a hora, por ejemplo se han observado fluctuaciones en un día de cambio de dólar a bitcoin del orden del 38%*), aun no son totalmente aceptados, dificultad a la hora de asociar una identidad a una *dirección bitcoin* (*posibilidad de tráfico ilegal*) [18], existencia de *incidentes de ciberseguridad*, las transac-ciones son irreversibles, es descentralizado, facilidad para enviar y recibir dinero, lo pueden utilizar países pequeños y débiles, la *PoW* crece en dificultad con el tiempo, utiliza *árbol Merkle* para guardar la historia de transac-ciones, etc.

Las ***transacciones bitcoin*** que se pueden observar ***actualmente*** son relativamente simples [14] (por ejemplo, *pagar con una clave pública una cantidad de bitcoins*), pero en el futuro cabe pensar en ***transacciones más complejas*** que permitan *pagar a cualquier entidad dentro de un grupo de varias entidades* o que sólo se pueda gastar si *K de N entidades firman* la transacción con sus claves privadas.

El *sistema de validación de transacciones* en *bitcoin* es muy flexible, aunque hoy en día no se explota todo su potencial. Pero cabe esperar que en un futuro próximo se soporten *transacciones más flexibles* y sofisticadas, podremos contemplar transacciones que contengan datos extra y *transacciones multiparte* complejas que utilicen la infraestructura que se emplea hoy en día.

El *ciberespacio* va siendo cada día más el protagonista número uno de nuevos ataques a los sistemas financieros a nivel global [19] y con respecto al *sistema bitcoin* ciertos ataques podrían afectar la cotización de la moneda *BTC*.

Por último cabe preguntarse si el *sistema bitcoin* representa el futuro de los sistemas de pago descentralizado a través de Internet (de cara al advenimiento de la *Economía Digital 3.0*) o sólo se trata de una burbuja que pueda terminar estallando, o quizás sea un sistema alternativo a los actualmente existentes [18][20].

El tiempo nos lo dirá. En cualquier caso su formulación técnica al día de hoy parece bastante robusta y flexible, incluyendo características de resiliencia importantes, y su comportamiento desde el punto de vista de su *ciberseguridad* es razonablemente aceptable.

Consecuentemente parece lógico afirmar que aún le queda bastante camino por recorrer. En el caso contrario (*siempre hay que tener en cuenta quién manda*), es muy probable que otros modelos similares e incluso híbridos lo releven y puedan continuar su camino ya iniciado.

Referencias

[1] J. Areitio. "Análisis de los problemas de seguridad-privacidad en e-Business/e-Commerce: Contramedidas". *Revista Española de Electrónica nº 689*, abril 2012.
[2] W. Kou. *Payment Technologies for E-Commerce*. Springer, 2010.
[3] J. Areitio. "Análisis de la protección del dinero electrónico para los negocios habilitados a través de Internet". *Revista Eurofach Electrónica nº 417*, marzo 2013.
[4] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". Prequel Books, 2011.
[5] Weusecoins. Vídeo sobre *qué es Bitcoin*, <http://www.weusecoins.com/>.
[6] The Bitcoin Channel. <http://www.thebitcoinchannel.com/>.
[7] J. Areitio. "Análisis de la protección de los sistemas de pago electrónicos en entornos e-Business/e-Commerce". *Revista Eurofach Electrónica nº 407*, marzo 2012.
[8] B. Rosenberg. "*Handbook of Financial Cryptography and Security*". Chapman and Hall / CRC, 2010.
[9] T. Mayer, B. Rounds. "*Bitcoin Beginner's Guide: Learn how to get started quickly and safely*". Premier Ark LLC, 2012.
[10]BayPay Forum. Red internacional de pago-comercio, <http://www.baypayforum.org>.
[11] BitPay. Proveedor de Servicios de Pago/ Pasarela de pago bitcoin P2P, <https://bitpay.com>.
[12] Bitcoinmail. Sitio que permite a los individuos enviar *monedas BTCs* (*Bitcoins*) a otros a través de correo electrónico, <http://www.bitcoinmail. com>.
[13] Bitcoin Monitor. Muestra las transacciones más recientes intercambiadas, <http://www.bitcoinmonitor.com>.
[14] Bitcoin Forum. <https://bitcointalk.org/>.
[15] J. Areitio. "*Seguridad de la Información: Redes, Informática y Sistemas de Información*". Cengage Learning-Paraninfo, 2013.
[16] Blockchain. Muestra gráficos y estadísticas de la economía global de bitcoin, <http://blockchain.info/charts>.
[17] Bitocoinity.org. Muestra gráficos de precios en tiempo real, <http://bitcoinity.org/markets>.
[18] K. Schurman. "*Bitcoin: Free Money or Fraud ?*". Hyperink, 2012.
[19] G. Kostopoulos. "*Cyberspace and cybersecurity*". Auerbach Publications, 2012.
[20] R. Amores, P. Paganini. "*Digital Virtual Currency and Bitcoins: The Dark Web Financial Markets-Exchanges and Secrets*". CreateSpace Independent Publishing Platform, 2013.

Notas

[1] En ingeniería de la seguridad, un *nonce* es un número arbitrario usando solamente una vez en comunicación criptográfica (traducción de <http://en.wikipedia.org/wiki/Cryptographic_nonce>).
[2] En <https://www.spendbitcoins.com/> se especifica un listado de comercios donde ya se aceptan directamente *bitcoins*. Véase así mismo <http://www.weusecoins.com/en/>.
[3] <https:mtgox.com/>. Así mismo en <http://bitcoincharts.com/charts/> se muestran gráticos asociados.
[4] En <http://ltc.block-explorer.com> se muestra el contenido de los *bloques bitcoin*.
[5] <http://www.h-online.com/security/news/item/Bitcoin-theft-half-a-million-dollars-gone-1261306.html>.
[6] <http://www.bit-coin.fr/crash-de-la-valeur-du-bitcoin-piratage-de-mtgox/>.
[7] <http://www.tribbleagency.com/?p=8133>.
[8] <http://www.launch.is/blog>.