revista digital universitaria
www.revista.unam.mx

1 de enero de 2017 | Vol. 18 | Núm. 1 | ISSN 1607 - 6079

ARTÍCULO

BITCOIN: UNA VISIÓN GENERAL

(http://www.revista.unam.mx/vol.18/num1/art11/)

Moisés Salinas Rosales
(Profesor en el CIC, IPN)
Victor Gabriel Reyes Maledo y
(Licenciado en Ingeniería Matemática con Línea Financiera, IPN)
Gina Gallegos Garcia
(Coordinadora del seminario de Seguridad y Criptografía en la ESIME)

1 de enero de 2017 | Vol. 18 | Núm. 1 | ISSN 1607 - 6079
http://www.revista.unam.mx/vol.18/num1/art11/

BITCOIN: UNA VISIÓN GENERAL

> Bitcoin es un sistema de pago electrónico que, por su arquitectura y forma de operar, tiene el potencial para ser implementado globalmente.

Resumen

Bitcoin es un sistema de pago electrónico que desde su aparición en 2009 se ha posicionado como uno de los de mayor uso, dando pie a que diversas empresas alrededor del mundo lo promuevan y adopten. Por ello resulta de gran valor para el público interesado en las nuevas tecnologías el poseer una visión general acerca de su funcionamiento y las implicaciones que su uso tiene en la actualidad. Este trabajo pretende aportar un panorama del sistema de pago *Bitcoin* describiendo su funcionamiento, arquitectura, modo de operación y algunas de las consideraciones financieras asociadas; se espera que este escrito pueda ser utilizado como una introducción para quien se encuentre interesado en el estudio del tema.

Palabras clave: *Bitcoin*, *e-payment*, minería, *blockchain*, *e-currency.*

Bitcoin: An Overview

Abstract

Bitcoin is an electronic payment system that since its appearance in 2009 has positioned itself as one of the most promoted and adopted by companies around the word, therefore it is of great value to the interested public to have general overviews of its operation and the implications that its use presents. This paper aims to provide an overview of the Bitcoin payment system describing its operation, architecture, the ways it operates and some of the associated financial considerations; it is hoped that this paper can be used as an introduction for anyone who is interested in studying the subject.

Keywords: *Bitcoin, e-payment, mining, blockchain, e-currency.*

BITCOIN: UNA VISIÓN GENERAL

Introducción

Bitcoin es un sistema de pago electrónico que inició operaciones en 2009 y que cuenta con una moneda digital propia,divisible hasta en cien millones de partes, programables e identificables, por lo cual resultan infalsificables, conocida como *bitcoin*[1] (BTC). Se caracteriza por estar construido con base en un protocolo criptográfico, con ello, ofrece un alto nivel de seguridad pues se ha observado resistente a fraude, falsificación, devoluciones[2] y otros ataques. Es un sistema distribuido (trabaja con una red de voluntarios) y descentralizado (no depende de una autoridad central, como gobiernos o bancos) por lo que permite llevar a cabo transacciones sin intermediarios (Nakamoto, 2008) haciendo que el costo de operación sea menor comparado con otros sistemas.

Bitcoin ofrece anonimato a sus usuarios de una manera similar a la forma en que lo hace el dinero en efectivo, debido a que las transacciones no están asociadas con datos personales.

Desde el punto de vista económico no presenta riesgo de inflación ya que su oferta está limitada, desde su diseño, a un total de 21 millones de unidades monetarias, mismas que son emitidas de manera paulatina (McCallum, 2014). Estas monedas no tienen valor per se, y no están respaldadas por una cantidad de algo o por algún servicio, por lo que son similares al dinero fiduciario actual. Su valor depende únicamente de la ley de oferta-demanda, lo que le otorga la ventaja de no verse afectado por políticas monetarias de bancos centrales. (De Filippi, 2014). Al igual que una moneda extranjera, un bitcoin puede ser comprado o vendido en casas de cambio, cajeros o con empresas que lo acepten como forma de pago. Aunque es posible usar este sistema como instrumento de inversión, puede ser riesgoso debido al alto nivel de volatilidad que presenta en su cotización. Hasta Noviembre de 2016, se reporta que hay cerca de 16 millones de bitcoins en circulación, es decir, aproximadamente 12 mil millones de dólares. En promedio, cada 24 horas se llevan a cabo 297 mil transacciones que en conjunto suman poco más de 1.6 millones BTC ("Bitcoin Charts / Bitcoin Network" 2016)

Actualmente, la validez y estatus legal de este sistema se debaten a nivel internacional, no obstante, en Japón se contempla su declaración como moneda de uso común, E.E.U.U. lo considera un commoditie -mercancía como el trigo y el petróleo- y México, Singapur, Alemania y Canadá han tomado una postura de espera. Por otro lado, China y Rusia han prohibido su uso.

Arquitectura del Sistema Bitcoin

La operación del Sistema Bitcoin se realiza con base en un conjunto de elementos que interactúan entre sí para integrar su arquitectura, tal como se ilustra en la Figura 1. A continuación se hace una descripción de dichos elementos:

- Los participantes: Desempeñan al menos uno de dos roles; el de usuarios mediante el intercambio comercial de bitcoins, y el de mineros mediante la validación de

[1] En este y otros textos se hace referencia al sistema como Bitcoin (con mayúscula) y a la moneda como bitcoin (con minúscula) representada por las siglas BTC.

[2] En términos sencillos, una devolución ocurre cuando un cliente desconoce una transacción hecha con su tarjeta de crédito. Entonces el banco responsable devuelve el dinero al cliente y hace un cargo contra el vendedor. Si bien el motivo más frecuente es el uso no autorizado de la tarjeta de crédito por terceros, se han detectado devoluciones fraudulentas en las cuales el cliente reclama la devolución de su dinero habiendo ordenado y recibiendo el producto o servicio en cuestión.

transacciones.

- Las transacciones: Es el intercambio de bitcoins entre usuarios. Para ello, hacen uso de sus monederos, llaves criptográficas y direcciones.
- El *blockchain*: Es el registro histórico de las transacciones que se han llevado a cabo en el sistema. Se organiza mediante bloques, que son conjuntos de direcciones.

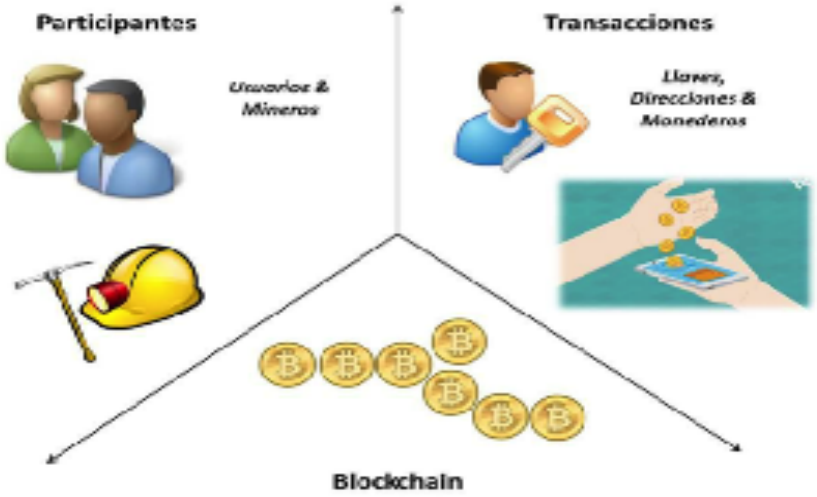

Figura 1 Arquitectura del Sistema *Bitcoin*

Participantes

Usuarios

Se denomina *usuario* al participante que usa *Bitcoin* con fines de intercambio comercial (medio de pago) o como depósito de valor (inversión), sin tener mayor influencia en el modo de operación del sistema.

Mineros

Bitcoin se basa en una red de colaboración (P2P) donde todos los participantes son iguales, es decir, comparten tareas y responsabilidades en el sistema. Los nodos de esta red son los *mineros*, y su tarea consiste en verificar las transacciones realizadas y dar validez a la operación del sistema.

El trabajo de los *mineros* comienza con la labor de agrupar las transacciones en un *bloque* para verificar su validez, es decir, comprobar la procedencia de las monedas para garantizar que no son falsificadas o que no hayan sido gastadas con anterioridad (prevenir el doble gasto). Una vez realizada esta verificación, cada uno intenta colocar el bloque sobre el cual está trabajando en el registro histórico de transacciones, llamado blockchain, y tendrá éxito en ello si logra resolver un problema matemático que propone el sistema. A esta actividad se le conoce como minería, y se describirá con detalles más adelante.

La motivación para que la red de mineros lleve a cabo esta labor radica en que el sistema emite una cantidad de monedas que asigna como pago a cada minero ganador, el cual será el primero en resolver el problema matemático y colocar su bloque en el *blockchain*. Esto se hace a manera de compensación por los recursos y el esfuerzo invertidos durante la minería, además es la forma en la que se controla la emisión de nuevas monedas. Cuando se iniciaron operaciones, en 2008, la recompensa era de 50 BTC, a partir de Noviembre del 2012 se redujo a 25 BTC y desde Julio de 2016 es de 12.5 BTC. De esta manera, cada 4 años se reduce el número de monedas emitidas hasta que el límite de 21 millones sea alcanzado.

Las transacciones

Una transacción en este sistema se define como el intercambio de la propiedad de un número determinado de *bitcoins*. En ella se indican al menos una dirección de origen (desde donde se toman los fondos), y al menos una dirección de destino (a donde se envían), así como el monto de la operación (Antonopoulos, 2014).

Direcciones

Figura 2 Código QR

Una *dirección Bitcoin* es una referencia que se utiliza para indicar al receptor de un pago, por lo que es necesario compartirla con otros usuarios de la red. Se representa como una cadena alfanumérica de entre 26 y 35 caracteres, que inician con 1 o 3, por ejemplo:

1PPVzjfPZece9mwJKdPB5Kbhv4JiSemFCu

También es común utilizar su representación como código QR[3], lo que resulta útil dado que al escanear dicho código se evita que el usuario cometa errores de captura. La Figura 2 muestra un ejemplo de cómo es un código QR.

Una *dirección bitcoin* puede visualizarse como una cuenta bancaria en la que se reciben depósitos y desde la que se hacen envíos de dinero. Las direcciones pueden ser generadas sin ningún costo ni límite, por lo que un usuario puede tener tantas direcciones como le sea necesario, y no serán asociadas con él dado que no se requieren datos personales para administrarlas. Cabe destacar, que, con el fin de mejorar el nivel de anonimato que el sistema es capaz de ofrecer, es recomendable generar una nueva dirección por cada pago que se reciba.

Llaves

Cada *dirección Bitcoin* tiene asociadas un par de llaves criptográficas: Una pública y una privada. La llave pública se utiliza para generar la dirección, e identificar con ello al receptor y al pagador en una transacción. Por otro lado, la llave privada se usa para que el pagador

[3] Un código QR es un código de barras bidimensional cuadrado que puede almacenar los datos codificados

autorice la transacción, de la misma manera en que lo hace la firma del titular de una cuenta en un cheque, es de suma importancia mantener en secreto la llave privada, de lo contrario, quien tenga posesión de ella tiene control sobre los fondos de la dirección correspondiente. En la actualidad estas llaves guardan compatibilidad con el estándar ECDSA[4].

Monedero

Es un dispositivo físico, sitio web, software o aplicación desde el que se administran las *direcciones Bitcoin*, y con el cual se envían y reciben pagos. Básicamente, consiste en una colección de llaves privadas que brindan al usuario acceso a sus direcciones asociadas.

La cadena de bloques

Es el registro histórico de todas las transacciones válidas que se han realizado desde la puesta en marcha del sistema *Bitcoin*; está organizado en bloques de transacciones (los bloques se describen más adelante), mismos que se van encadenando uno tras otro. Se considera que la cadena de bloques (*blockchain*) es el equivalente a un libro contable, donde todas las operaciones están disponibles para ser consultadas por el público.

Las transacciones quedan confirmadas en la medida que los bloques son añadidos al *blockchain*, es decir, una vez que fue añadido todas las transacciones incluidas en éste se consideran exitosas. Procesar y añadir un bloque toma en promedio 10 minutos. Es posible que se produzcan ataques al sistema intentando deshacer una transacción, sin embargo si dicha transacción está contenida en un bloque al que ya se han encadenado otros seis, el ataque es virtualmente infructuoso debido a la capacidad de procesamiento que sería necesaria para llevarse a cabo. En otras palabras, se considera que una transacción está completamente asegurada después de una hora de llevarse a cabo.

Dado que los mineros compiten por añadir su propio bloque, no es raro que varios de ellos coincidan en reportarlos minados al mismo momento, lo que conlleva que el *blockchain* incorpore dichos bloques como candidatos, creando una ramificación. Ante esta situación el bloque a añadirse en forma permanente se definirá a partir de la rama en la cual se logre minar el siguiente bloque de transacciones. En consecuencia los bloques descartados quedan *huérfanos* y sus transacciones vuelven a la red para ser reprocesadas. El primer *bloque de Bitcoin* generado desde el inicio de su operación es conocido como *bloque génesis*. Esta situación se describe en la Figura 3, donde el bloque génesis es representado por la letra G. Luego, del bloque 1 al 7 se observa la ruta principal de la cadena. En las ramificaciones, el minero ganador decide dónde añadir el siguiente bloque y la cadena continuará por esa rama, que presenta mayor trabajo de cómputo, dejando en calidad de huérfanos a los bloques descartados.

[4] Firma Digital con base en Curvas Elípticas, descrito por el NIST FIPS 186-4.

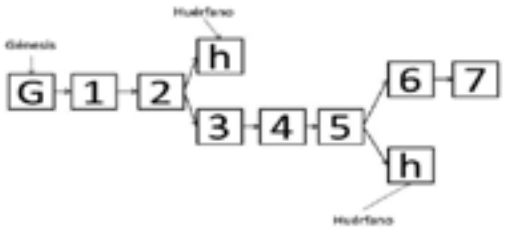

Figura 3 Bifurcación del blockchain

Los bloques

Cuando un usuario genera una transacción, esta se envía a un *pool*[5] de transacciones a la espera de ser validadas. De allí los mineros las toman a discreción y agrupan junto con otras tantas para integrar estructuras conocidas como *bloques*, que son el equivalente a las hojas de un libro de contabilidad, donde se guardan todas las transacciones de un período[6]. Un *bloque* consta de una cabecera y un conjunto de transacciones. Su estructura se muestra en la Figura 4:

Figura 4 Estructura de un bloque

Como puede observarse, la información que conforma un bloque está organizada en campos, los cuales se describen a continuación:

- *Versión*: Indica la versión del formato del bloque. El formato actualmente es 2 y cualquier bloque con diferente versión es rechazado.
- *Hash del bloque previo*: Es un identificador del último bloque minado en la cadena, al cual se añade el nuevo. Técnicamente se conoce como *resumen criptográfico*. Se expresa mediante una cadena de caracteres de longitud fija.
- *Raíz del Árbol de Merkle*: *Resumen criptográfico* que representa la información de todas las transacciones que se incluyen en el bloque. Se expresa mediante una cadena de caracteres de longitud fija.
- *Timestamp*: Indica la fecha y hora en que el bloque fue añadido al *blockchain*.
- *Bits*: Indica la condición del problema matemático que se pretende cumplir para validar las transacciones del bloque.
- *Nonce*: Indica el valor aleatorio único utilizado durante el proceso de minería para resolver el problema matemático.
- *Número de transacciones*: Indica el total de transacciones que constituyen el bloque.
- *Vector de Transacciones*: Lista a detalle de las transacciones incluidas en el bloque.

[5] Del verbo en inglés *pool*, que significa poner en un fondo común.

[6] En la página web www.blockchain.info es posible visualizar en tiempo real la generación de bloques y su estructura.

Los *resúmenes criptográficos* empleados en el sistema son una herramienta que permite verificar la integridad de las transacciones en caso de que se presente un ataque cuyo objetivo sea alterar la información del *blockchain*; dado que los bloques están encadenados, cualquier intento por modificar la información obligaría a modificar los resúmenes criptográficos, lo cual es poco factible debido a que con la capacidad de procesamiento de las computadoras actuales un ataque requeriría años (cientos o miles) para tener éxito.

¿Cómo opera *Bitcoin*?

Los pagos en *Bitcoin* son la transferencia de propiedad sobre las monedas digitales entre dos o más usuarios. Esta se reflejará en los monederos de los usuarios. Suponga que dos usuarios, Alice y Bob, van a realizar una transacción, donde Alice debe pagar a Bob una cantidad de bitcoins. Los pasos a seguir son los siguientes:

1. Bob indicará a Alice una dirección. Si decide usar una nueva dirección, debe generarla en el monedero. De lo contrario, puede indicar una previamente generada.
2. Alice debe abrir la aplicación de monedero en su teléfono móvil, e ingresar la dirección que Bob le indicó (manualmente o escaneando el código QR) y el monto que desea pagar en los campos respectivos.
3. Alice seleccionará la opción *enviar* para hacer el pago.
4. Deberán esperar la confirmación del pago. Actualmente una confirmación toma cerca de 10 minutos.

Una cada vez que se realiza un pago desde una dirección, los fondos de esta serán extraídos en su totalidad, por lo que en el caso de que los fondos transferidos resulten mayores que el pago deseado, será necesario indicar una dirección propia para recibir la diferencia o cambio (los monederos actuales realizan este proceso de manera automática).

> Por ejemplo, si Alice debe enviar 6 BTC a Bob, y en su monedero tiene una dirección que contiene 10 BTC, debe enviarlos en dos partes, indicando al monedero la dirección de Bob donde enviar 6 BTC y una dirección propia para recibir los 4 BTC correspondientes al cambio.

¿Cómo y dónde puedo comprar *bitcoins*?

Para iniciar la compra y venta de *bitcoins*, o bien para hacer pagos mediante este sistema, es necesario adquirir un monedero para administrar las direcciones y los fondos. Éste se puede descargar de forma gratuita a un dispositivo como un teléfono inteligente, una tableta, o una computadora. Para comparar algunas opciones y elegir la más conveniente de acuerdo con el perfil del usuario, se recomienda visitar el sitio:

https://bitcoin.org/es/elige-tu-monedero

Posteriormente se pueden adquirir *bitcoins* mediante alguna de las siguientes formas:

- **Mediante minería**: El sistema paga cierta cantidad de bitcoins y comisiones a los mineros que validan un bloque, sin embargo, esto requiere una fuerte inversión en equipo de cómputo.
- **Compra entre usuarios**: Es posible pagar a otro usuario en efectivo el valor de determinada cantidad de *bitcoins* para que dicho usuario haga la transferencia correspondiente.
- ***Cajeros Bitcoin***: Si la ciudad en la que reside el usuario cuenta con el servicio de *cajero Bitcoin*, debe dirigirse a este e ingresar el monto en efectivo correspondiente a la cantidad de *bitcoins* que desea adquirir de acuerdo con el tipo de cambio vigente al momento de la transacción, así como ingresar en la pantalla del cajero una *dirección Bitcoin* de su propiedad en la que recibirá dichos fondos.

Una forma alternativa es a través de empresas financieras especializadas en el sistema, que además de ofrecer el servicio de monedero también permiten realizar operaciones de comercio, de forma similar a una bolsa de valores, que hace lo propio con las acciones de algunas empresas. Para ello, es necesario registrar una cuenta en alguna de estas empresas y asociarla con una cuenta bancaria. La cuenta bancaria servirá para financiar la compra de bitcoins y, en su caso, para recibir el efectivo correspondiente a la venta de los mismos. Algunas empresas mexicanas que ofrecen este servicio son *Volabit*[7] y *Bitso*[8].

> Por ejemplo, si Alice debe enviar 6 BTC a Bob, y en su monedero tiene una dirección que contiene 10 BTC, debe enviarlos en dos partes, indicando al monedero la dirección de Bob donde enviar 6 BTC y una dirección propia para recibir los 4 BTC correspondientes al cambio.

Comisiones

Se paga una comisión al minero que procese una transacción, esta se calcula como la diferencia entre la cantidad indicada a pagar y la cantidad de bitcoins disponible en las cuentas de origen de donde se tomarán los recursos. En el ejemplo anterior, puede indicarse al monedero que a la dirección propia, la que se usa para recibir el cambio, regrese solo 3.5 BTC. Así, del total de fondos que tenía Alice, 10 BTC, se transfirieron a las cuentas especificadas 9.5 BTC (6 BTC por pagar y 3.5 BTC de cambio) por lo que la diferencia, 0.5 BTC queda como comisión al minero, de ahí que se recomienda -si se desea agilizar la validación del pago- establecer una comisión que sea un buen incentivo para los mineros. En el momento en que se hayan emitido los 21 millones de *bitcoins* establecidos como tope, esta será la única forma en que los mineros obtendrán ganancias monetarias por su trabajo. La comisión mínima por defecto es de 0.0001 BTC.

[7] https://www.volabit.com/es

[8] https://www.bitso.com

Minería de las transacciones y prueba de trabajo

Como se dijo anteriormente, la minería es el proceso de verificar y dar validez a las transacciones recientes, para lo cual es necesario invertir poder de cómputo para procesar transacciones y así garantizar la seguridad de la red.

En particular, para que las transacciones recientemente generadas sean confirmadas, el proceso de minería del sistema incorpora el concepto de prueba de trabajo (Back, 2002), que consiste en la solución de un reto matemático que propone el sistema. Este reto consiste en un problema difícil de resolver que requiere hacer un gran número de cálculos por segundo. Los mineros realizan el procesamiento necesario para intentar resolver el reto y así lograr que sus bloques sean aceptados en la cadena y con ello poder recibir la recompensa que se ofrece.

La prueba tiene dos propiedades básicas, asegura que se invirtió tiempo para generarla y por lo tanto para verificar la validez de las transacciones y es fácilmente verificable.

¿En qué consiste la prueba?

Básicamente, se trata del algoritmo de un protocolo criptográfico que debe dar como resultado un valor determinado por el sistema. Este algoritmo toma como entradas los datos correspondientes al bloque (estos datos están descritos en la sección los *bloques*) y, dado que es un proceso determinista –las mismas entradas siempre producen las mismas salidas- toma como elemento de aleatoriedad un número llamado *nonce*, el cual será variado tantas veces como sea necesario para obtener el resultado que pide el sistema.

El planteamiento de este problema permite que el sistema ajuste la dificultad de manera que se mantenga el promedio de 10 minutos para que sea solucionado.

Debido al carácter competitivo en el proceso de minería, es importante el equipo de cómputo que se tenga disponible. Por ello si bien en un principio era suficiente con una computadora promedio, hoy en día los recursos dedicados a la minería de transacciones han evolucionado pasando por el uso de GPUs[9] hasta llegar al uso de circuitos FPGAs[10] e incluso al uso de ASICs[11] diseñados exclusivamente para minar *bitcoins* y que representan hoy la opción eficiente en términos de ahorro de electricidad y menor generación de calor.

Además, con el fin de concentrar más poder de procesamiento, los mineros han comenzado a organizarse en grupos llamados *pool's*, que agrupan la capacidad de minería de cada uno de sus integrantes, y al resolver el reto, se reparten la recompensa en forma proporcional a lo que cada uno colaboró.

Contexto actual *Bitcoin*, México y el FMI

En México, ya existen empresas que aceptan esta forma de pago. Y otras tantas que funcionan como operadoras de Bitcoin, varias de ellas mexicanas y que ofrecen la posibilidad de comprar, vender e invertir en esta moneda digital. Al cierre de este artículo, el tipo de cambio[12] era de:

[9] Son unidades de procesamiento de gráficos de alto desempeño, utilizadas originalmente para video juegos y animación por computadora.

[10] Son circuitos programables que ofrecen un muy alto desempeño por realizar todo el procesamiento en hardware directamente.

[11] Los dispositivos ASIC son circuitos integrados diseñados a medida para realizar una función específica que por lo reglar ofrecen un desempeño superior a los FPG`As.

[12] www.bitso.com Consultado el 05 de Diciembre de 2016 a las 13:59 hrs

1 BTC = $16279.23 MXN

El uso de esta tecnología en nuestro país como medio para intercambiar valores no está prohibido. No obstante, está restringido -al igual que el dinero en efectivo- para llevar a cabo transacciones sensibles al lavado de dinero. Esto significa que no se permite usar *bitcoins* para comprar inmuebles, autos a partir de cierto monto, obras de arte, recepción de donativos, prestación de servicios de comercio exterior, etc. La lista de actividades y los montos máximos permitidos antes de ser considerados actividades vulnerables se pueden consultar en la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (SEGOB, 2013). Al respecto, el Banco de México ha declarado que esta tecnología no representa un riesgo al sistema financiero mexicano ni a los sistemas de pagos pues el volumen de uso actual no es relevante, en este sentido, se ha limitado a advertir al público sobre los posibles riesgos y a declarar que emitirá la regulación correspondiente cuando lo juzgue necesario (Banco de México, 2014).

En el contexto global, el Fondo Monetario Internacional (FMI) afirma que esta moneda electrónica combina distintas propiedades del dinero fiduciario, *commodities* y sistemas de pago, por lo que no puede ser clasificada dentro de ninguna de estas opciones y requiere un tratamiento específico de acuerdo a sus características Aun así, concluye que el sistema sigue siendo un desarrollo joven y que es muy pronto para saber a dónde se dirige (Criptonoticias, 2016).

Problemas abiertos de *Bitcoin*

Existen dos tipos de problemas relacionados con el uso de *Bitcoin* como sistema de pago. El primer tipo tiene que ver con las actividades ilícitas que se ven favorecidas con las características de anonimato propias del sistema, cuyo efecto inmediato es un alto grado de dificultad para rastrear las transacciones, a diferencia de otros sistemas de pago electrónico. Esto deriva en el uso del sistema como medio de pago en mercados negros dentro de la *deep web*[13], donde a cambio de *bitcoins* es posible adquirir armas, financiar grupos terroristas o lavar dinero. Un caso famoso fue el de Silk Road, un sitio de comercio de sustancias ilegales que fue cerrado por el FBI en 2013 (Ron&Shamir, 2014).

Otro caso de actividades ilícitas que involucra a al sistema como medio de pago es el *ransomware*, el cual se ha posicionado como una de las mayores amenazas informáticas hoy en día. Se trata de un *malware* que bloquea equipos conectados a Internet o bien, cifra la información que estos resguardan y exige al usuario el pago de un rescate a cambio de su liberación. Este pago generalmente se pide en *bitcoins*, por lo que incluyen tutoriales sobre el manejo de esta moneda. Si el usuario no paga, el atacante amenaza con eliminar sus archivos de manera permanente.

El segundo tipo de problema con el sistema está relacionado con la facilidad con la que estos, como cualquier otra pieza de información electrónica, puede ser robado, lo cual aunado a la falta de infraestructura de las organizaciones que se dedican a comercializar con esta moneda, o que proveen servicios de monedero, puede derivar en grandes pérdidas ante el incidente de un ataque informático. En este sentido en múltiples ocasiones ya se ha reportado el robo de cantidades importantes. El más reciente tuvo lugar en Agosto de 2016 en la plataforma de comercio Bitfinex, donde luego de detectar

[13] La *deep web* es un conjunto de sitios web y bases de datos a los cuales los buscadores comunes no tienen acceso ya que no están indexadas. El contenido que se puede hallar dentro de la internet profunda es muy amplio, e incluye diversas actividades ilegales.

una brecha de seguridad se informó del robo de 119,756 BTC con un valor cercano a los 67 millones de dólares (Bitfinex, 2016). Otro caso importante fue el de MtGox, una de las operadoras más importantes de *Bitcoin* en el mundo y que perdió 850 mil *bitcoins* con valor cercano a los 370 millones de dólares debido a una falla de seguridad entre los años 2013 y 2014 (De Filippi, 2014).

Con la introducción de este sistema dentro de las organizaciones, y aún más en la generación de nuevos modelos de negocio, es necesario dar seguimiento a la evolución de las implicaciones que esta tiene para poder prevenir la aparición de escenarios de abuso de la tecnología, tanto aquellos que la afectan directamente, como aquellos donde ésta se torna en un facilitador de dicho abuso, como es el caso de los delitos.

Conclusiones

Bitcoin es un sistema de pago electrónico que, por su arquitectura y forma de operar, tiene el potencial para ser implementado globalmente. Entre sus *ventajas* destaca la integridad del sistema la cual no descansa sobre personas o instituciones, sino sobre procedimientos matemáticos que han probado ser eficientes y seguros, que resuelven problemas comunes, como la falsificación y el del doble gasto, a través de la validación de las transacciones por medio de la red de mineros. Esto implica el hecho de que no hay forma de cometer fraude o modificar las *reglas del juego* sin contar con el consenso de la red. Aunado a esto, el hecho de que las unidades monetarias son infalsificables puede llevar a este sistema a ser considerado una alternativa al dinero físico, como ha ocurrido en Japón. Además, el límite de 21 millones de unidades previene el fenómeno de inflación. Por otra parte, es una alternativa para hacer pagos y enviar dinero por todo el mundo de forma libre, sin horarios, sin bancos, con completo control y con comisiones muy bajas.

Más aún, debido al esquema de recompensas y comisiones con el que los mineros reciben un pago por sus servicios, muchas personas han visto en dicha actividad una oportunidad de negocio redituable, lo cual aporta cierto grado de auto-sustentabilidad. Entre sus desventajas se encuentra su precio altamente volátil, ya que ha demostrado fuertes variaciones como respuesta a las reacciones de ciertos sectores, en particular, ha bajado de precio cuando un gobierno declara su uso como prohibido o cuando una operadora sufre un ataque. Además son pocos los negocios pequeños que lo aceptan como medio de pago; se espera que cuánto más difundido sea su uso más estable se vuelva su precio.

En lo que respecta a las investigaciones en un aspecto técnico, estas se han centrado en comprender la dinámica de las redes de *Bitcoin*, haciendo intentos por vencer el anonimato –área en la cual ya hay avances (Spagnuolo 2014)- y combatir las malas prácticas como lavado de dinero y fraude, toda vez que dichas prácticas han generado un estigma social hacia este sistema, sin embargo, es importante recordar que no son exclusivas del sistema, ya que el dinero en efectivo es igualmente utilizado para fines ilícitos.

Bibliografía

[1] ANTONOPOULOS, Andreas M. Mastering Bitcoin: unlocking digital cryptocurrencies. [en línea]. Estados Unidos: O'Reilly Media, 2014. Disponible en: http://uplib.fr/w/images/8/83/Mastering_Bitcoin-Antonopoulos.pdf

[2] BACK, Adam. Hashcash- A denial of service counter-measure. [en línea]. 2002. Disponible en: http://www.hashcash.org/hashcash.pdf

[3] Banco de México. Información para la prensa [en línea] 2014. Disponible en: goo.gl/HJyt6z [Consulta: 18 Agosto 2016].

[4] Bitcoin network. Bitcoincharts.com. [en línea] 2016. Disponible en: http://bitcoincharts.com/bitcoin/ [Consulta: 05 de Diciembre 2016].

[5] Bitfinex: The official blog. [en línea]. 2016. Disponible en: http://blog.bitfinex.com/uncategorized/security-breach/ [Consulta: 20 Agosto 2016]

[6] DE FILIPPI, Primavera. Bitcoin: a regulatory nightmare to a libertarian dream. Internet Policy Review journal on internet regulation. [en línea]. 2014, vol. 3, no 2. Disponible en: https://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

[7] Handbook of applied cryptography. Alfred J. Menezes; Paul C. van Oorschot; Scott A. Vanstone (eds). Boca Raton, Florida : CRC Press, 1996. 780 p. ISBN: 0-8493-8523-7

[8] HERNÁNDEZ, Ariana. Fondo Monetario Internacional publica informe acerca de Bitcoin y la Blockchain. Criptonoticias. [en línea] [citado enero 22 del 2016]. Disponible en: http://criptonoticias.com/regulacion/fondo-monetario-internacional-publica-informe-acerca-de-bitcoin-y-la-blockchain/#axzz4II0bJT9k [Consulta: 15 Agosto 2016]

[9] HERRERA-JOANCOMARTÍ, Jordi. Research and Challenges on Bitcoin Anonymity. En Data privacy management, autonomous spontaneous security, and security assurance : 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014 : revised selected papers. Cham : Springer, 2015. 3-16 p. ISBN: 9783319170169

[10] Ley Federal para a prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. [en línea[.SEGOB, Publicada DOF (16/08/2013), 2013. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf

[11] MCCALLUM, Bennett T. Bitcoin Issues: Shadow Open Market Committee Meeting. [en línea]. Economic Policies for the 21 st Century at the Manhattan Institute. 2014. Disponible en: http://shadowfed.org/wp-content/uploads/2014/10/McCallumSOMC-November2014.pdf

[12] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. [en línea]. 2008. Disponible en: https://bitcoin.org/bitcoin.pdf

[13] RON, Dorit., SHAMIR, Adi. How did dread pirate roberts acquire and protect his bitcoin wealth?. En International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014. 3-15. ISBN: 978-3-662-45471-8

[14] Secure Hash Standard (SHS).Department of ommerce United States of America.[en linea]. March 2012. Disponible en: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[15] SPAGNUOLO, Michele., MAGGI, Federico., ZANERO, Stefano. Bitiodine: Extracting intelligence from the bitcoin network. En International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014. 457-468P . ISBN: 978-3-662-45471-8