



UNIVERSIDAD
NACIONAL
DE TUCUMÁN



FACULTAD DE
CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL TUCUMAN

BITCOIN, LA MONEDA DIGITAL

Autores: Díaz, Carmen Cecilia
Lozano Aráoz, Adriana Lucía
Yáñez, Nirvana María Noelia

Director: Rearte, Susana

2016

Trabajo de Seminario: Contador Público Nacional

RESUMEN

El presente trabajo de seminario consistió en investigar sobre el *Bitcoin, la moneda digital*.

Siendo el bitcoin un tema que aún resulta bastante complejo de explicar a quienes conocen muy poco o desconocen totalmente del mismo, nuestro desafío se presentó, una vez identificados los conceptos básicos y elementos que intervienen en el sistema, en lograr una explicación ordenada y lo más simple posible sobre de que se trata esta moneda virtual.

Para ello organizamos el trabajo en una introducción y tres capítulos, a saber:

- Capítulo I: ¿Qué es el bitcoin?
- Capítulo II: ¿Qué es el bitcoin?
- Capítulo III: Desafíos del bitcoin

PRÓLOGO

Desde los albores de la Historia, el dinero en cualquiera de sus múltiples formas ha sido necesario para el funcionamiento de las sociedades desarrolladas.

El dinero, esta palabra tan habitual, se puede definir como todo aquello que podemos usar normalmente para hacer pagos. El término en sí deriva de *denarius*, nombre latino de una importante moneda romana de plata, y por extensión es sinónimo de riqueza en general.

Al inicio de la historia no existían monedas ni billetes para pagar los bienes o servicios. Los hombres utilizaban el trueque como forma de intercambio de productos o servicios, es decir, que canjeaban cosas u horas de trabajo por otras cosas o tareas que necesitaban para sus vidas. Más tarde, conforme las sociedades se desarrollaron, las necesidades aumentaron, por lo cual se hizo necesario que existiera un medio de intercambio más práctico y cómodo que el trueque. Al principio se utilizaron granos de cacao, ostras, sal o metales preciosos, como el oro o la plata. Más adelante, surgió la necesidad de que el medio de intercambio fuera más eficiente.

Por esta razón se inventó la moneda metálica y un poco más tarde, el billete o papel moneda, los cuales son:

- ✓ Duraderos, es decir, soportan pasar de mano en mano y se mantienen en buen estado durante un tiempo razonable.
- ✓ Transportables, esto es, tienen el tamaño ideal para llevarse de un lugar a otro sin dificultad.
- ✓ Divisibles, lo que significa que con ellos se paga con gran exactitud el precio de cualquier mercancía.
- ✓ Homogéneos. Esto es, que todas las monedas o los billetes de la misma denominación valen lo mismo.
- ✓ Tienen aceptación obligatoria, que significa que todas las personas los deben utilizar dentro de nuestro país para pagar o cobrar.

El dinero tiene además las siguientes propiedades:

- Es unidad de cuenta, lo que permite fijar los precios de los bienes y servicios. Sin él no sabríamos cuánto cuestan.
- Es un medio de pago, ya que es aceptado por todas las personas para pagar la compra y venta de los bienes y servicios.
- Es depósito de valor, lo que quiere decir que conserva su valor en el tiempo, pues tiene la capacidad de comprar bienes y servicios en el futuro.

Desde principios del siglo XX van desapareciendo los metales preciosos en las acuñaciones y después de la Segunda Guerra Mundial el papel moneda predomina sobre la moneda, ahora sujeta a normas internacionales, y realizada en aleaciones sin valor. La moneda queda relegada a un papel de apoyo en el sistema monetario.

Entre las diferentes formas de dinero que utilizamos actualmente, cabe destacar en especial las monedas y los billetes, aunque también utilizamos a menudo los cheques, las letras de cambio y las tarjetas de crédito. Otros objetos más modestos de nuestra vida cotidiana como fichas o tarjetas telefónicas, bonos de transportes, fichas-monedas, vales-billetes o tarjetas de uso interno en casinos, comercios, grandes almacenes, etc., también son dinero, por lo que vemos que la gama es tan amplia como permite y garantiza la ley.

La historia del dinero aún no ha terminado, pues en el futuro habrá, sin duda, nuevas formas de pago de la mano de la revolución electrónica e informática aportando nuevos conceptos de dinero.

INTRODUCCIÓN

Bitcoin es una moneda electrónica descentralizada concebida en el año 2009. Se entiende por “**moneda digital**, (también conocido como cripto-moneda, ciber-moneda, dinero digital, e-moneda, dinero electrónico, e-dinero) el dinero que sólo se transfiere por medios electrónicos. Cuando se producen las transferencias de dinero como una transferencia bancaria, o incluso las transferencias de dinero a través de servicios tales como PayPal, los fondos se envían por vía electrónica, pero lo que se transmite es dinero representado en una moneda fiduciaria subyacente.”⁽¹⁾



El nombre **Bitcoin** se aplica también al software libre diseñado por **Satoshi Nakamoto** para su gestión y a la red P2P de la que consta. Satoshi

⁽¹⁾ Consultas en Internet: https://es.bitcoin.it/wiki/Moneda_electr%C3%B3nica

Nakamoto es el creador de Bitcoin y el desarrollador inicial del **cliente original de Bitcoin**, el Bitcoin, que es un programa que implementa el protocolo Bitcoin para su uso desde línea de comandos y mediante llamadas de procedimientos remotos (es también el primer cliente de Bitcoin en la historia del sistema, y debido a su condición de primer cliente de Bitcoin escrito por Satoshi Nakamoto se le designa habitualmente como "cliente de Satoshi", también se le llama el "cliente de referencia", por tratarse de la implementación de referencia funcional para cualquier otro cliente). Volviendo a Satoshi Nakamoto, se sabe muy poco sobre él y su identidad real. Estuvo implicado en el proyecto Bitcoin desde el año 2007. Su participación en el proyecto Bitcoin se fue reduciendo y concluyó a finales de 2010.

Al contrario que la mayoría de las monedas, Bitcoin no depende de la confianza en ningún emisor central, sino que recurre a una base de datos distribuida en varios nodos de una red P2P para registrar las transacciones y utiliza la criptografía para proveer funciones de seguridad básicas, tales como garantizar que las bitcoins solo puedan ser gastadas por su dueño, y nunca más de una vez.

El diseño de Bitcoin permite poseer y transferir valor en la forma potencialmente anónima. Las monedas pueden ser guardadas en cualquier ordenador en la forma de un archivo "de bolsillo", o con un tercero que ofrezca el servicio de almacenar ese archivo. En cualquiera de los casos, los bitcoins pueden ser enviados por medio de Internet a cualquiera que tenga una "dirección Bitcoin". La estructura P2P de Bitcoin y la falta de administración central hace imposible para cualquier autoridad, gubernamental u otra, la manipulación del valor de los bitcoins o la creación de inflación produciendo más de ellos.

Bitcoin es una nueva moneda experimental que está en desarrollo activo. Aunque cada vez es menos experimental al crecer su uso, se debe tener en cuenta que Bitcoin es una nueva invención que está explorando ideas que nunca antes se han intentado. Como tal, su futuro no se puede predecir por nadie.

CAPITULO I

¿Qué es Bitcoin?

Sumario: 1.- Introducción. 2.- Diferentes maneras de obtener Bitcoin. 3.- Respaldo y valor de Bitcoin. 4.- Emisión de Bitcoin. 5.- Elementos del sistema. 6.- Ventajas del Bitcoin. 7.- Desventajas del Bitcoin.-

1.- Introducción:

Bitcoin es una innovadora red de pagos y una nueva clase de dinero.

El Bitcoin es pionero en la implementación de un concepto llamado criptomoneda expuesto por Dai Wei en 1998 cuyo fundamento es que el dinero es un objeto, o cualquier tipo de registro, aceptado como pago de bienes y servicios, y el pago de las deudas en un determinado país o contexto socioeconómico.

Esta moneda que nació en 2009 permite a los usuarios intercambiar créditos en línea por bienes y servicios.

Como se mencionara anteriormente, Bitcoin usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos. La gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. Por lo tanto, Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet.



Bitcoin es de código abierto, su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar. De la misma manera que nadie controla la tecnología detrás del correo electrónico, Bitcoin tampoco tiene propietarios. Bitcoin lo controlan todos los usuarios de Bitcoin del mundo. Aunque

los programadores mejoran el software, no pueden forzar un cambio en el protocolo de Bitcoin porque todos los demás usuarios son libres de elegir el software y la versión que quieran. Para que sigan siendo compatibles entre sí, todos los usuarios necesitan utilizar software que cumpla con las mismas reglas. Bitcoin sólo puede funcionar correctamente si hay consenso entre todos los usuarios. Por lo tanto, todos los usuarios y programadores tienen un gran incentivo en proteger dicho consenso.

Por medio de sus muchas propiedades únicas, Bitcoin permite usos interesantes no contemplados por ningún sistema de pagos anterior.

2.- Diferentes maneras de obtener Bitcoin:

La criptomoneda se obtiene de diversas maneras:

- ✓ Se los puede comprar: existen sitios específicos para el intercambio de divisas con Bitcoin
- ✓ Se los puede aceptar como moneda de cambio al vender bienes: existen sitios de subastas donde se venden artículos con esta divisa
- ✓ También pueden obtenerse apostando: existen varios sitios de apuestas que aceptan la criptomoneda como pago de las apuestas
- ✓ Pero la manera más genuina de emitir Bitcoins se lleva a cabo online (en algunos sitios de Internet especializados) mediante la realización de ciertas tareas por intermedio de una computadora, proceso conocido como mining (minería). Las cantidades que se emiten están controladas por los programadores informáticos que trabajan a través de algoritmos. Minar datos significa que se generan automáticamente bajo un proceso de transacciones sin controles con algoritmos matemáticos complejos para evitar que cualquiera emita una cantidad indefinida.

3.- Respaldo y valor de Bitcoin:

El respaldo de Bitcoin son sus cualidades monetarias, basadas en las inmutables leyes de la matemática. La moneda no produce riqueza. La buena moneda

es necesaria para que los recursos sean adecuadamente aprovechados, pero a la riqueza la producen los individuos interactuando libre y voluntariamente.

El precio de un Bitcoin se determina como todo en Economía, por su oferta y su demanda. Cuando la demanda de los Bitcoins incrementa, el precio incrementa, y cuando la demanda baja, el precio baja, por eso de momento el precio del Bitcoin es muy volátil en la actualidad.

Dado que el valor del Bitcoin se desprende exclusivamente de la oferta y la demanda, el precio debería subir para satisfacer una demanda creciente, teniendo en cuenta que las cantidades de moneda en el mercado están controladas: existe un máximo de bitcoins que se emitirán y a partir de ahí ya no habrá bajo los estándares actuales una mayor emisión, lo que les reviste de una característica única, la de la oferta futura invariante. No se sabe cuándo ya que dependerá del ritmo de emisión.

4.- Emisión de Bitcoin:

El límite de 21.000.000 de Bitcoins que impone el protocolo es arbitrario. Lo que importa es que, de acuerdo a las reglas que aceptan implícitamente todos los que utilizan el sistema, ese límite no puede ser superado, ni puede alterarse el ritmo en que se incrementa la masa monetaria. En este sentido, Bitcoin es absolutamente previsible, algo fundamental para un sistema monetario.

Los bitcoins son generados como una recompensa al trabajo de los mineros, y dicha recompensa disminuye a la mitad cada 4 años. Hacia el año 2030 se habrán generado casi todos los bitcoins que llegarán a existir, aunque lo cierto es que seguirán generándose (cada vez menos) bitcoins. A la larga sólo ingresarán a la economía pequeñas fracciones de un Bitcoin (cada vez menores) en el curso de varios años, pero la curva que representa el aumento de la masa monetaria continuará acercándose asintóticamente a 21.000.000.

La escasez de bitcoins nunca va a ser un problema, porque cada Bitcoin puede dividirse hasta el octavo decimal, y potencialmente aún más. Es decir que hoy puedes pagarle a alguien la cantidad de 0,00000001 Bitcoin. Hablamos de una masa monetaria total integrada por, como mínimo, cuatrillones de unidades, así que

bastaría un sólo Bitcoin en circulación para abastecer de suficientes unidades monetarias a todo el planeta. En el futuro, de ser necesario, las unidades en uso podrían pasar a llamarse microbitcoins, nanobitcoins, etc.



5.- Elementos del sistema:

- Balances – Cadenas de bloques
- Transacciones – Llaves privadas
- Procesamiento – Minería

Balances – Cadena de bloques

La cadena de bloques o "block chain" es una contabilidad pública compartida en la que se basa toda la red Bitcoin. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos Bitcoin pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se está haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con criptografía.

Transacciones – Llaves privadas

Una transacción es una transferencia de valores entre monederos Bitcoin que será incluida en la cadena de bloques. Los monederos Bitcoin disponen de un fragmento secreto llamado *clave privada*, utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La *firma* también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios y por lo general empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de un proceso llamado *minería*.

Procesamiento – Minería

La minería es un sistema de consenso distribuido que se utiliza para *confirmar* las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas en un *bloque* que se ajuste a estrictas normas de cifrado y que será verificado por la red. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

La minería casi nunca fue muy rentable para los que liquidan inmediatamente los bitcoins minados: al principio, por ejemplo, uno podía llegar a obtener cientos de bitcoins en un día de minería, pero no había manera de venderlos por más de USD 0,0001 (o ni eso). La minería sólo es rentable para los que entienden los fundamentos de Bitcoin, y por ende creen en el brillante futuro de esta tecnología. Así que todo depende del horizonte temporal del minero.

La probabilidad de adquirir bitcoins por medio de la minería depende de muchos factores, el principal de los cuales es el poder computacional que aporta el total de los mineros. La dificultad se ajusta automáticamente cada diez días para que el incremento de la masa monetaria ocurra según el ritmo programado.



El sistema está diseñado para que la generación de bloques ocurra más o menos cada diez minutos, sin importar la cantidad de transacciones que cada bloque incluya. Más transacciones, de todas maneras, no significan necesariamente más trabajo para el minero. Y aunque en el futuro se van a generar menos bitcoins, hay que tener en cuenta que la misma restricción del incremento de la masa monetaria podría condicionar un aumento en el precio del bitcoin.

6.- Ventajas del Bitcoin:

- **Global:** no pertenece a ningún estado o gobierno y se puede utilizar en todo el mundo, independientemente de las barreras geográficas y políticas.

- **Ajeno al sistema fiduciario:** no se puede crear deuda con él, su valor no depende de una intervención de un banco central.
- **Límite de emisión:** el aumento decreciente y predecible de la masa monetaria, le permite mejorar el poder adquisitivo de los usuarios.
- **Moneda divisible:** actualmente se puede utilizar hasta con 8 decimales aunque no hay límite por lo que en un futuro se podrían utilizar más decimales.
- **Transacciones en tiempo real:** en menos de una hora puede estar realizada la transacción.
- **Irreversibilidad de las transacciones:** no hay un tercero en medio que pueda echar atrás una transacción. De todos modos existen servicios que custodian los bitcoins hasta que la parte que los recibe ha cumplido con su parte del acuerdo.
- **Imposible de falsificar:** tal como está definido no se puede construir un bitcoin falso ni efectuar un doble gasto sin que la red lo detecte.
- **No hay un regulador:** ningún comité de “expertos” controla el destino del bitcoin. Hay unas reglas previamente fijadas por el protocolo ideado por Satoshi Nakamoto que ha de aceptar libremente quien quiera utilizar el bitcoin.
- **Anonimato:** nadie está obligado a revelar su identidad lo que hace al bitcoin especialmente útil para su uso en países donde gobiernan regímenes totalitarios.
- **Barato:** el bitcoin tiene menores costes de transacción que la utilización de tarjetas de crédito, transferencias o Paypal. Realizando un pago con bitcoin se eliminan intermediarios no deseados.
- **Seguro:** el bitcoin cuenta con un fuerte respaldo criptográfico que lo protege de falsificaciones y se puede guardar en múltiples localizaciones simultáneamente. La tecnología en la que se basa el protocolo del bitcoin es varias veces más segura que la que utilizan los bancos y las tarjetas de crédito.

- **Transparencia:** todas las transacciones quedan grabadas en un registro de libre acceso.
- **Micropagos:** dado su divisibilidad y sus bajos costes de transacción es una moneda ideal para realizar micropagos.
- **Funciona las 24 horas al día:** para las operaciones en **bitcoins** no existen horarios ni días festivos.
- **Se acumula en un espacio ínfimo:** podría guardarse una fortuna enorme en una memoria USB, que puede ser guardada o trasladada sin depender de terceros.

7.- Desventajas del Bitcoin:

- **Límite de emisión.** Si bien es positivo para evitar la pérdida de valor, el que sea deflacionaria podría incentivar su acumulación y por tanto como dice el premio Nobel de Economía Paul Krugman podría deprimir la economía.
- **Volatilidad:** desde su creación ha tenido grandes subidas de precio. El 2013 lo empezó a 10,2 EUR/BTC y lo cerró a 579,9 EUR/BTC, llegando cerca de los 900 EUR/BTC, lo que hace del bitcoin una moneda atractiva para la especulación. Con el tiempo lo normal es que el porcentaje de variación se reduzca y tenga una cotización más estable.
- **Garantía de aceptación:** aunque cada vez hay más establecimientos que los aceptan todavía son una minoría. Es utilizado fundamentalmente por *feelances* y para la adquisición de material informático.
- **No hay un regulador:** el que no tenga un respaldo detrás de gobiernos y bancos centrales para muchos puede ser una clara desventaja ya que se sentirían más cómodos con el apoyo de un regulador.
- **Anonimato:** al igual que en el punto anterior, la enorme ventaja que supone el que las transacciones sean anónimas es una desventaja para

- 14 -

muchos que temen que sea utilizada para actividades ilícitas y para no cumplir con las obligaciones tributarias.

CAPITULO II

¿Cómo usar Bitcoin?

Sumario: 1.- Introducción. 2.- Uso de Bitcoin. 3.- Elección de monedero. 4.- Obtención de Bitcoin. 5.- Gasto de Bitcoin. 6.- Transformar Bitcoin en dinero.-

1.- Introducción:

Desde la perspectiva del usuario, Bitcoin no es más que una aplicación móvil o de escritorio que provee un monedero Bitcoin personal y permite al usuario enviar y recibir bitcoins con él. Así es como funciona Bitcoin para la mayoría de los usuarios.

Un usuario nuevo puede empezar con Bitcoin sin entender los detalles técnicos. Una vez usted instalado un monedero en la computadora o dispositivo

móvil, se generará la primera dirección Bitcoin y se podrá crear más cuando se necesite. Se puede dar la dirección a contrapartes para que paguen o viceversa. De hecho, es similar a como funciona el correo electrónico, excepto que las direcciones Bitcoin solamente deberían ser usadas una única vez.

Detrás de las cámaras, la red Bitcoin comparte una contabilidad pública llamada "block chain". Esta contabilidad contiene cada transacción procesada, permitiendo verificar la validez de cada transacción. La autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío, permitiendo a todos los usuarios tener control total al enviar Bitcoins desde sus direcciones Bitcoin. Además, cualquiera puede procesar una transacción usando el poder computacional de hardware especializado y conseguir una recompensa en Bitcoins por este servicio. Esto es comúnmente llamado "mining" o minería.

2.- Uso de Bitcoin:

Utilizar Bitcoin y operar con ellos es tan sencillo como enviar un correo electrónico. Cualquiera que disponga de una dirección Bitcoin podrá enviar o recibir Bitcoin a otro usuario que también tenga otra dirección.

Cada usuario cuenta con una dirección que es con la que se identifica con el resto de los usuarios y es una dirección pública, es decir, cualquier persona que conozca esa dirección Bitcoin podrá enviarle Bitcoins. Al igual que cualquier cuenta de correo electrónico, la cuenta Bitcoin de un usuario dispondrá también de una clave privada que es la que permite realizar envíos de Bitcoins o acceder a la propia cuenta Bitcoin.

Las contraseñas están altamente protegidas por contraseña cifrada. El sistema utilizado para los Bitcoins confía totalmente en el poder de los números y ese es su punto fuerte.

Bitcoin es diferente de lo que se conoce y usa todos los días. Bitcoin le permite intercambiar dinero de forma diferente a como se lo hace normalmente en el banco.

Para realizar un seguro y correcto uso de Bitcoin es recomendable entender en qué consisten las siguientes acciones:

- ❖ Elección de monedero
- ❖ Obtención de Bitcoin
- ❖ Gasto de Bitcoin
- ❖ Transformar Bitcoin en dinero

3.- Elección de monedero:

Para tener Bitcoin es necesario disponer de un monedero donde guardarlos. Un monedero es una aplicación disponible tanto para computadora como para móviles, y también están los monederos web.

Se puede usar un monedero Bitcoin en la vida cotidiana con un dispositivo móvil o se puede tener un monedero solo para pagos online desde la computadora.

Al igual que en la vida real, el monedero debe estar protegido. Bitcoin permite transferir dinero a cualquier lugar fácilmente y permite tener el control sobre su dinero. Estas grandes características también conllevan riesgos de seguridad. Al mismo tiempo, Bitcoin ofrece altos niveles de seguridad si se usa correctamente.

Un monedero Bitcoin es como un monedero con dinero real. Por el mismo motivo que no se guardaría grandes cantidades en efectivo en el bolsillo, se tiene que tener el mismo cuidado con el monedero Bitcoin. En general, es aconsejable tener en el ordenador, móvil o servidor sólo pequeñas cantidades para uso diario y tener el resto de los fondos en un lugar más seguro.

Si se guarda en un lugar seguro, la copia de seguridad de un monedero puede proteger contra fallos de la computadora o humanos. También permite recuperar el monedero si se sufre el robo del móvil o computadora, siempre que el monedero se encuentre encriptado.

La encriptación del monedero o Smartphone permite establecer una contraseña para cualquiera que intente retirar fondos. Esto ofrece protección contra el robo, aunque no ofrece protección contra sistemas de software o hardware de "keylogging".

Un monedero offline, también conocido como almacenamiento en frío, ofrece el mayor nivel de seguridad para los ahorros. Este sistema consiste en guardar el monedero en un lugar seguro y que no esté conectado a Internet. Cuando se realiza correctamente, este sistema ofrece muy buena protección contra las vulnerabilidades de una computadora. El uso de un monedero offline junto con copias de seguridad y encriptación también es muy seguro.

Los bitcoins de un usuario se pueden perder para siempre si no tiene un plan de respaldo para persona allegadas o familiares. Si la ubicación de los monederos o sus claves no son conocidas por nadie cuando ya no esté, los fondos no podrán ser recuperados.

4.- Obtención de Bitcoin:

Se puede obtener bitcoins aceptándolos como pago por bienes y servicios o comprando a un tercero. También se puede comprarlos directamente desde una casa de cambio a través de una cuenta bancaria.

El precio de un Bitcoin es impredecible, puede aumentar o disminuir en un corto período de tiempo debido a su joven economía, su carácter novedoso y en ocasiones mercados ilíquidos. Por lo tanto, mantener ahorros en Bitcoin no es recomendable. Bitcoin se debe considerar como un activo de alto riesgo, y nunca se debe almacenar dinero que no se pueda permitir el lujo de perder con Bitcoin. Si se recibe pagos con Bitcoin, muchos proveedores de servicios permiten convertirlos instantáneamente en moneda local.

5.- Gasto de Bitcoin:

Hay un creciente número de servicios y comerciantes aceptando Bitcoin en todo el mundo. Se puede usar Bitcoin para pagarles y valorar su experiencia para ayudar a que los negocios con esta modalidad ganen más visibilidad.

En Argentina ya hay hoteles, cafetería, locales de comidas rápidas e incluso plataformas de comercio electrónico que aceptan pagos en Bitcoin, incluso

con descuentos especiales ya que por esas transferencias no se pagan las comisiones de servicios financieros o tarjetas de crédito.

6.- Transformar Bitcoin en dinero:

Con respecto a cómo convertir la criptomoneda en dinero corriente existen muchas formas de hacerlo.

La primera, la más común, es usar directamente alguna casa de cambio virtual que realice estas transacciones, que permite cambiar bitcoins por dólares sin cobrar comisión alguna. A diferencia de muchas otras exchanges (sobre todos las que se han creado para países de América Latina), Circle es una casa de cambio virtual que paga en dólares la cantidad correcta por los bitcoins que le son vendidos.



Una segunda opción es vender los bitcoins directamente a otras personas. Aunque pueda parecer difícil, existen grupos en redes sociales como Facebook en el que distintos usuarios recomiendan a otros usuarios a los que les han vendido o comprado bitcoins. Con esto sin duda hay que tener cuidado y saber a quién venderle, aunque sin duda es una opción viable puesto que entre las dos personas se ponen de acuerdo a qué tasa van a vender o comprar estas criptomonedas.

Una tercera opción es no cambiar bitcoins a dólares sino usarlos directamente para comprar productos y servicios. La idea de usar bitcoin es dejar de depender de las monedas nacionales.

Existen, por supuesto, muchos exchanges y servicios de compra/venta de bitcoin.

CAPITULO III

Desafíos del Bitcoin

Sumario: 1.- Introducción. 2.- Bitcoin y lavado de dinero.
3.- Bitcoin y ciber-crimen.-

1.- Introducción:

El avance de Bitcoin plantea que la moneda virtual puede terminar siendo también un sistema de pago muy eficaz para enviar remesas entre países, y no sólo para transacciones de comercio electrónico.

Para las autoridades mundiales será un dolor de cabeza si se mantiene como mecanismo que no cuenta con las normas para evitar el **lavado de dinero** y la **financiación del terrorismo**. También, el Bitcoin enfrenta el reto que supone el **ciber-crimen**. El crimen y los malwares generalmente siguen el trayecto del dinero, y las cryptodivisas son la nueva sensación del mundo cibernético.

2.- Bitcoin y lavado de dinero:

Los controles de capitales quedan desafiados por el Bitcoin.

Es evidente que las monedas virtuales no solo plantean actualmente una amplia gama de riesgos de lavado de dinero que son propias de su sector, sino que además agravan los desafíos del lavado de dinero más tradicional, que las instituciones financieras enfrentan hoy en día. El principal desafío para la industria de la moneda virtual es su naturaleza anónima, que permite a los criminales participar en los mercados financieros y convertir, transferir y retirar los fondos sin detección.

Las dificultades que plantea el anonimato se ven exacerbados por la facilidad en el movimiento de fondos a través de fronteras, y la velocidad a la que opera la industria. Los desafíos de identificación de las actividades sospechosas y la actividad de seguimiento de clientes aumentan significativamente cuando el anonimato protege la identidad del cliente, dificulta la identificación de las fuentes de los fondos y el propósito económico de la transacción.



El hecho de que el anonimato prospere en el mundo virtual significa que los reguladores y la industria en general tendrán que gestionar el riesgo inevitable de facilitar el blanqueo de dinero y las actividades delictivas.

Por lo tanto, las instituciones financieras y cambiarias que proporcionan el vínculo entre las monedas tradicionales y virtuales también tendrán que considerar si sus sistemas y controles existentes para prevenir y detectar el lavado de dinero siguen siendo aptos para el propósito de encarar esta industria emergente. Asimismo, debe continuamente monitorearlos a medida que la industria evolucione en el futuro.

3.- Bitcoin y ciber-crimen:

Los ciberdelincuentes encuentran más que atractivas para su negocio a las transacciones electrónicas. Hasta la aparición del Bitcoin en el 2009, los delincuentes asumían el riesgo de utilizar la intermediación financiera para transferir los beneficios ilícitos obtenidos. Como forma de ocultación, abrían cuentas bancarias con identidades y documentación falsa o robada y se exponían físicamente o se registraban vía online de modo que el que gestionaba las altas no podía contrastar la documentación enviada con la identidad real.

Posteriormente vinieron los sistemas prepago o de tarjetas prepagadas tipo cupones que permite pagar sin la mediación de cuentas bancarias ni tarjetas de crédito. Únicamente tienes que adquirir unos cupones prepagados e introducir el código pin que llevan asociado y todo eso sin que por medio conste un nombre y apellidos. Western Union, Moneygram o Paypal son otra forma anónima de pagar y dificultar más aún la trazabilidad del dinero online.

Aun con la utilización de documentación falsa o robada, cuentas bancarias extranjeras en paraísos fiscales, y otra clase de artimañas para dificultar y dilatar tanto las investigaciones, en la mayoría de los casos se han permitido centrar las investigaciones y llegar a sus autores.

Actualmente la población mundial es víctima del **ransomware**, aquella infección que cifra el disco duro de la víctima o bloquea el acceso al sistema y que

impide el acceso de la víctima a su ordenador. Este malware tiene ahora una forma de cobro seguro: el Bitcoin.

¿Por qué se piden los rescates en Bitcoin? Su anonimato o cuasi anonimato les hace ser muy atractivos para los delincuentes. Pueden ser transferidos de forma ágil y rápida y no hay control ni intermediación financiera. Al no estar bajo ningún control, tampoco hay un registro de las direcciones.



CONCLUSIÓN

Ya varios comercios aceptan pagos con Bitcoins: su masividad hará subir su precio. Aquí cuatro motivos deberían ser suficiente para compensar los riesgos de obtener, almacenar y transferir o pagar con Bitcoins por los bienes y servicios en el día a día. Motivos suficientes también para un inversor para especular sobre su precio:

- En primer lugar porque permite rápidas operaciones entre pares
- En segundo lugar porque permite efectuar pagos en todo el mundo
- En tercer lugar porque las comisiones son muy bajas o inexistentes
- En cuarto lugar porque su emisión está limitada a un máximo fijo en el tiempo

Además de su poder transaccional, su uso principal podría ser en el futuro una reserva de valor, aunque no tengan un valor intrínseco. No es una alternativa al oro *per se*, pero muchos han estado comprándola como reserva de valor a futuro.

En síntesis, si bien la aceptación y la reserva de valor son dos de las características centrales de cualquier divisa en las cuales el bitcoin ha avanzado mucho, el respaldo y la seguridad son dos puntos no menores en los cuales deberá trabajar a futuro para poder sustituir a otras monedas.

El futuro de este sistema nuevo de moneda digital es aún incierto, si bien se augura que puede ser el más seguro a utilizar en la red, ya que estamos bastante familiarizados con causas de fraude de dinero en la red.

Este sistema al estar perfectamente encriptado y descentralizado promete ser una revolución y alternativa a las tarjetas de crédito por ejemplo, pero aún queda un largo camino por recorrer. Quizás sea aún más corto que el que venimos recorriendo con las tarjetas de crédito, que prácticamente las utilizamos para todo, pero el sistema Bitcoin pretende ser mucho más seguro, transparente a todos los usuarios y neutral, sin que haya bancos ni instituciones privadas detrás.

Un aspecto sumamente importante será el rol de las instituciones financieras y cambiarias que proporcionan el vínculo entre las monedas tradicionales

y virtuales que tendrán que considerar si sus sistemas y controles existentes para prevenir y detectar el lavado de dinero son aptos para tal fin. Asimismo, deberán ser continuamente monitoreados a medida que la industria evolucione en el futuro.

APENDICE

¿Quién creó Bitcoin?

El fantasma de Satoshi Nakamoto, uno de los mayores misterios de la era digital.

Bitcoin es la primera implementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai en la lista de correo electrónico "cypherpunks", donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada. La primera especificación del protocolo Bitcoin y la prueba del concepto la publicó Satoshi Nakamoto en el 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin.

La anonimidad de Satoshi a veces ha levantado sospechas injustificadas, muchas de ellas causadas por la falta de comprensión sobre el código abierto en el que se basa Bitcoin. El protocolo Bitcoin y su software se publican abiertamente y cualquier programador en cualquier lugar del mundo puede revisarlo o crear su propia versión modificada del software. Al igual que los programadores actuales, la influencia de Satoshi se ha limitado a que los cambios que hizo los adoptaran los demás y, por tanto, no controlaba Bitcoin. Así, conocer la identidad del inventor del Bitcoin es igual de relevante que saber quién inventó el papel.

ÍNDICE BIBLIOGRÁFICO

A) ESPECIAL

Consultas a bases de información, en Internet:

www.es.bitcoin.it/wiki/Moneda_electr%C3%B3nica

Consultas a bases de información, en Internet:

www.elbitcoin.org/

Consultas a bases de información, en Internet:

www.bitcoin.org/es/

Consultas a bases de información, en Internet:

www.bitcoinargentina.org/

B) OTRAS PUBLICACIONES

Consultas a bases de información, en Internet:

http://www.abc.es/tecnologia/informatica/software/abci-bitcoin-entre-experimento-fallido-y-revolucion-201601250222_noticia.html

Consultas a bases de información, en Internet:

<http://www.abc.es>

Consultas a bases de información, en Internet:

<http://eleconomista.com.mx/fondos/2015/03/11/abc-bitcoin-explosion-burbuja-depuracion-consolidacion>

ÍNDICE

	<u>Pág.</u>
PRÓLOGO	1.-
INTRODUCCIÓN	3.-

CAPÍTULO I

¿Qué es Bitcoin?

1.- Introducción.....	5.-
2.- Diferentes maneras de obtener Bitcoin.....	7.-
3.- Respaldo y valor de Bitcoin.....	7.-
4.- Emisión de Bitcoin.....	8.-
5.- Elementos del sistema.....	9.-
6.- Ventajas del Bitcoin.....	11.-
7.- Desventajas del Bitcoin.....	13.-

CAPÍTULO II
¿Cómo usar Bitcoin?

1.- Introducción.....	15.-
2.- Uso de Bitcoin.....	16.-
3.- Elección de monedero.....	17.-
4.- Obtención de Bitcoin.....	18.-
5.- Gasto de Bitcoin.....	18.-
6.- Transformar Bitcoin en dinero.....	19.-

CAPÍTULO III
Desafíos del Bitcoin

1.- Introducción.....	21.-
2.- Bitcoin y lavado de dinero.....	22.-
3.- Bitcoin y ciber-crimen.....	23.-

CONCLUSIÓN.....	25.-
APÉNDICE.....	27.-
ÍNDICE BIBIOGRÁFICO.....	29.-
ÍNDICE.....	30.-