

Bitcoin como alternativa transversal de intercambio monetario en la economía digital

Bitcoin Transversal Alternative Monetary Exchange in the Digital Economy

Zully Julieth Palacios Cárdenas¹ Miguel Andrés Vela Avellaneda²
Giovanny Mauricio Tarazona Bermúdez³

Para citar este artículo: Palacios, Z.J., Vela, M.A. y Tarazona, G.M. (2015). Bitcoin como alternativa transversal de intercambio monetario en la economía digital. *Redes de Ingeniería*, 6(1), 106-128.

Recibido: 15-mayo-2015 / **Aprobado:** 15-junio-2015

Resumen

Bitcoin es un sistema de dinero digital descentralizado que está amenazando el uso del dinero convencional. Este sistema ha aumentado su popularidad atrayendo la atención de los medios, la comunidad y los organismos de control, dado su anonimato y estructura, donde los usuarios son quienes generan la moneda y verifican que las transacciones sean efectuadas por medio de un proceso criptográfico. El artículo evidencia el estado de arte de las diferentes formas de dinero que ha utilizado el ser humano, desde la aparición del trueque a partir del 9000 a.C, hasta llegar al Bitcoin como forma de dinero digital en la última década. Para el desarrollo de la investigación se hizo una búsqueda con las palabras: dinero (money), historia del dinero (history of money) y Bitcoin, principalmente en las bases de datos de las revistas: IEEE, ScienceDirect, Jstor-Journal Storage y Business Source Complete, de la Universidad Distrital Francisco José de Caldas y de la Universidad Nacional de Colombia (SINAB), donde se encontraron 355 documentos pero se seleccionaron 162 que favorecieron la revisión.

Finalmente se concluye que el Bitcoin es considerado como una moneda experimental por lo tanto carece de reconocimiento dentro de la economía global, pero a futuro puede ser una alternativa a los costosos sistemas tradicionales, logrando aumentar el acceso de los negocios en la red.

Palabras clave: Bitcoin, criptomoneda, dinero digital, dinero, historia del dinero, minería Bitcoin.

Abstract

Bitcoin is a decentralized system of digital money that is threatening the use of conventional money. This system has increased in popularity attracting media attention, community and control bodies, given their anonymity and structure where users are who generate the currency and verify that transactions are carried out by means of a cryptographic process. The article demonstrates the state of art of different forms of money used humans, since the emergence of barter from 9000 BC until the Bitcoin as a form of digital money in the last decade. For the development of research, it was searched

1. Estudiante de Ingeniería Industrial, Universidad Distrital Francisco José de Caldas. Contacto: zully_2792@hotmail.com
2. Estudiante de Ingeniería Industrial, Universidad Distrital Francisco José de Caldas. Contacto: mava305.a@gmail.com
3. Ingeniero Industrial, Universidad Distrital Francisco José de Caldas; doctor en Sistemas Informáticos para Internet, Universidad de Oviedo, Asturias, España; docente de la Universidad Distrital Francisco José de Caldas. Contacto: gtarazona@gmail.com

with the words: money (money), history of money (history of money) and Bitcoin, mainly in databases of journals: IEEE, ScienceDirect, JSTOR-Journal and Storage Business Source Complete the District University Francisco Jose de Caldas and the National University of Colombia (SINAB) where 355 documents were found but 162 of them were selected because favored the review. Finally we conclude that Bitcoin is considered an experimental currency therefore lacks recognition within the global economy, but the future can be an alternative to expensive traditional systems, achieving increasing access network business

Keywords: Bitcoin, criptocurrency, digital money, history of money, minning Bitcoin, money.

su ordenador o teléfono inteligente en cualquier parte del mundo a través de la red de forma segura. Bitcoin permite intercambiar dinero sin ningún intermediario, facilitando la transparencia de las transacciones con la ayuda de la criptografía de las firmas digitales, la cual da la posibilidad de validar y almacenar todas las transacciones públicamente. Los costos generados por la utilización de dinero en efectivo han sido altos (transporte, seguridad, impresión), e incluso los riesgos al transportarlo. Los anteriores factores han influido para que se desarrollen nuevos sistemas que faciliten las transacciones y se reduzcan los costos [3].

Bitcoin va más allá del alcance de dinero en efectivo, permitiendo transacciones globales procesadas en la misma velocidad que las locales. Al mismo tiempo, se debe considerar que es la única moneda en el mundo cuyo valor está regulado ciento por ciento por la ley de oferta y demanda. Pero existe un inconveniente para que este sistema de intercambio comercial tenga éxito, y es el de garantizar plena confianza, lo que implica reconocimiento por parte de gobiernos e instituciones financieras a nivel mundial. Es así como el estudio se centra puntualmente en analizar Bitcoin como alternativa transversal de intercambio en los mercados mundiales.

En primer lugar se aborda el concepto de dinero y se hace una revisión de los diferentes elementos que el ser humano ha utilizado como forma de intercambio, comenzando con el uso de materiales naturales hasta llegar a la aparición del dinero electrónico en la Sección 2. Posteriormente, en la Sección 3, se presenta al Bitcoin como una alternativa de dinero electrónico junto con sus generalidades y sus riesgos. Seguidamente, en la Sección 4, se muestra el proceso de transacción con Bitcoin. Más adelante en la Sección 5, se explica cada una de las partes que interactúan en el protocolo Bitcoin. En la Sección 6, se exponen una serie de eventos relacionados a ataques, robos y la

1. INTRODUCCIÓN

Internet World Stats afirma que para finales del año 2000 el número de usuarios de internet en el mundo era de 361 millones mientras que para junio de 2014 esta cifra había alcanzado los 3.035 millones, es decir el 42,3 % de la población mundial [1]. Por tanto, el paso de la economía tradicional a la economía digital ha sido posible con la revolución de internet, y como consecuencia los modelos de negocio han evolucionado por el desarrollo de nuevas tecnologías, nuevas formas de intercambio, o bien, el uso de nuevas unidades de cambio o monedas digitales. Es usual que la emisión de dinero sea responsabilidad de los bancos centrales y podría ser inconcebible desafiar esta premisa.

En el año 2008 surge la moneda digital descentralizada Bitcoin [2], creada probablemente por un seudónimo y utilizada para apoyar el comercio electrónico, permitiendo a los usuarios con acceso al internet realizar transacciones mediante

volatilidad que ha experimentado el Bitcoin desde sus inicios, para continuar con la Sección 7, donde se razonan una serie de ventajas y desventajas tanto desde el punto de vista económico-financiero como el funcional. Finalmente, en la Sección 8 se evidencia el reconocimiento y aceptación por parte de organismos internacionales hacia el Bitcoin, para terminar con las conclusiones y futuros temas de estudio en la Sección 9.

1. LA EVOLUCIÓN DEL DINERO EN LA HISTORIA

Como lo mencionan Cuervo, Reina, Zuluaga, Rozo, Santana y Echeagaray, el dinero es definido como un medio u objeto de intercambio socialmente aceptado, una representación abstracta de un valor respaldada por una autoridad y generalmente admitida para la realización de intercambios comerciales universales. Sin embargo, el dinero también es considerado no solo como un asunto económico, sino que también está profundamente relacionado a aspectos sociales, psicológicos y hasta políticos [4]-[6]. Dentro de este mismo contexto, Surowiecki, Bustamante, Escoto, *et al.*, lo definen por las tres funciones que desempeña en una economía: como medio de cambio, unidad de cuenta y reserva de valor, todas ellas relacionadas con la compra y venta. Las mismas conllevan a que el dinero nunca sea suficiente, y que la sociedad haga de su obtención su única meta en la vida [7], [8].

Históricamente una gran variedad de materias primas han servido en un momento u otro como dinero [9]. Por ejemplo, los nativos de ciertas regiones de la India utilizaban almendras, los guatemaltecos el maíz, los antiguos asirios y babilonios la cebada, los pueblos de Filipinas, Japón, Birmania y otras regiones del sudeste asiático tradicionalmente usaron el arroz como dinero [10]. Animales vivos, tabaco, cacao [11], pieles, aceite de oliva, licores, conchas marinas, piedras, dientes e incluso esclavos

y esposas, también sirvieron como medio de pago por los distintos bienes recibidos a cambio [12], [13]. Así, a partir de 9000 a.C se utilizó la ganadería y los productos agrícolas para facilitar el comercio, y se le nombró a esta actividad: el trueque. En este intercambio no existía un precio y no era posible distinguir entre comprador y vendedor [14].

Posteriormente en el siglo VII a.C, al descubrirse el metal y dificultarse el comercio del trueque, el Reino de Lidia en Asia menor emitió las primeras monedas hechas por conglomerados de electrón (aleación natural de oro y plata sacados de ríos de la zona) cortados en pequeños trozos. Tenían un peso determinado y eran selladas con una marca oficial para garantizar el valor, atribuyéndole a este reino la innovación de imprimir en las caras de la moneda. Las monedas se fabricaron con un peso y tamaño estándar para reducir el riesgo de engaños con la cantidad o calidad de oro y plata que utilizaban para realizar los intercambios [15]. Godazgar y Haddadi [16], se centran en la historia del oro y la plata como formas de dinero.

Años después estas monedas se perfeccionaron por los griegos, quienes hicieron de su invención una época que se denominó la Edad de Oro de Grecia (500 a 400 a.C); animales, objetos naturales y dioses griegos eran usados como símbolos en monedas griegas [17]. Después de la caída del Imperio Romano en el año 476 d.C, Europa se desestabilizó, por lo que había pocos gobiernos fuertes que podrían emitir dinero de una manera fiable. Como resultado, el dinero se vio difícil de conseguir y el comercio disminuyó [18]. Los anteriores hechos conllevan a que surgiera por primera vez en China el papel moneda en el año 650 d.C. con materiales manejables, económicos y variados diseños [19]. Inicialmente los europeos no adoptaron esta moneda, aunque era más fácil transportar papel que pesadas bolsas de monedas. Estos primeros "billetes" eran pedazos en forma cuadrada de piel de ciervo blanco con bordes de colores [20].

Más tarde, con el surgimiento del Renacimiento y la Revolución Industrial alrededor de 1300 d.C, los italianos crearon los bancos [18], [21]; y perfeccionaron el papel moneda, el cual se emitió para que lo utilizara diariamente el comercio. A mediados del siglo XV aparecen las letras de cambio, permitiendo el envío de dinero a distancia sin correr riesgos, así como los pagarés, las obligaciones o bonos, las acciones, los cheques y los giros postales [22]. Los billetes de papel se ataron al oro solo hasta 1816, y la Ley de Patrón Oro fue promulgada oficialmente en los Estados Unidos en 1900, lo que condujo al establecimiento de la Reserva Federal. De esta manera, el papel moneda estaba respaldado por metales preciosos, mediante un certificado que podía ser canjeado por su equivalente en metales preciosos en cualquier momento a quien lo recibiera en el intercambio [5].

Para el siglo XIX el mundo llegó a operar por primera vez bajo un único sistema monetario, basado en el valor de la divisa mundial: el oro [10]. Después de la Primera Guerra Mundial, el patrón oro se vio amenazado y la mayoría de países suspendieron la convertibilidad de su moneda en este metal. En los años treinta con la llegada de la Gran Depresión en todo el mundo [20], y más tarde la Segunda Guerra Mundial, se pone fin a la “regla de oro” así como al acuerdo de Bretton Woods: el patrón oro fue revisado y el precio del oro devaluado [23]. En 1971, EE.UU. canceló unilateralmente la convertibilidad directa del dólar estadounidense con el oro, que supuso el fin del acuerdo de Bretton Woods, así como el Gold Standard. El rápido desarrollo en todo el mundo desde esta fecha se considera como la prueba de la estabilidad del sistema financiero “dinero fiat” (sin el respaldo de oro) [16]. Este fue el primer paso para poner fin a la relación entre el oro y la moneda, lo cual marcó el comienzo de una compleja regulación monetaria internacional [20].

En el siglo XIX surgen los bancos centrales, definidos por el Banco de la República como aquellas

entidades establecidas en la capital de cada país encargadas de la emisión de moneda nacional bajo el resguardo del Banco Mundial y del Fondo Monetario Internacional [24]. Junguito y Ayala dan a conocer las etapas históricas del Banco Central a nivel mundial [25]. En resumen, la invención del papel moneda acabó con el feudalismo, e hizo descender la base del poder económico desde la propiedad de tierras, a la de mercados bursátiles, acciones, y corporaciones. De este modo, a mediados de los años noventa la relación deja de ser bilateral y se pasa al dinero plástico, en forma de tarjetas de pago. Según Rockwell y el Banco de la República, las tarjetas de pago han tenido como característica común el hecho de poseer uno o más hologramas y un bloque de firma (para la firma del titular de la tarjeta), así como una banda magnética, que permite la codificación de los datos del mismo [26], [27].

Existen tres tipos de tarjetas de pago, las cuales se diferencian por el tiempo entre pagos y la transacción. El primero es la tarjeta de crédito con la cual el portador puede disponer de una cuenta de créditos por parte de la entidad que la emite, para ser utilizada en los establecimientos afiliados. Con su sola presentación se puede posponer el cumplimiento de las obligaciones financieras asumidas (las cuales deben ser reembolsadas junto con los intereses) [10]. El segundo tipo es la de débito, la cual se emplea para realizar pagos en los establecimientos que la aceptan como medio de pago. La operación se registra en la cuenta y el valor de la compra se descuenta automáticamente de la cuenta bancaria el dinero que en realidad posee y puede disponer [28]. Y el tercero es la tarjeta prepagada o monedero electrónico, la cual permite hacer compras en cantidades reducidas: se compran por un valor específico y con éstas se realizan gastos hasta que el dinero acumulado se acabe.

En Estados Unidos surgen las primeras tarjetas emitidas en gasolineras, posteriormente se adoptan por

cadenas de almacenes y finalmente, Diner's Club crea en 1950 la primera tarjeta de crédito hecha de cartón, con el nombre del cliente en una cara y un listado de los restaurantes miembros al reverso. Para 1955, Diner's Club ya contaba con una tarjeta hecha de plástico [29]. Al existir un nuevo producto financiero que amenazaba con quitarles el control crediticio de montos relativamente bajos a los bancos, estos decidieron crear sus propias tarjetas de crédito plastificadas. En 1958 el primero en crear una tarjeta de este tipo es el banco estadounidense "Bank of America", denominada BankAmericard. En seguida, se unieron al sistema BankAmericard pequeños bancos para tener su propia tarjeta.

En 1967 el banco neoyorquino City Bank, introdujo al mercado su tarjeta de crédito llamada Everything Card, conocida mundialmente como "MasterCard" Posteriormente en 1977, la denominada BankAmericard cambió su nombre por "Visa", haciendo una difusión importante de sus tarjetas de crédito (logrando ser la más popular para 1990) [30]. Esta forma de concebir el dinero incentivó el consumo así como los servicios, la producción y el PNB, pero lo hizo al costo de un alto endeudamiento individual y de una inflación internacional [29].

Posteriormente, con la invención de la tarjeta inteligente (smart card o chip card), nace la concepción de dinero electrónico [31]. Las tarjetas inteligentes se diferencian de las demás tarjetas de pago porque poseen un microchip de computador en el cual almacenan una mayor cantidad de información que las tarjetas con bandas magnéticas, permitiendo hacer transferencias de fondos de una manera más eficiente, razón por la cual pueden tener más usos [32]. La acreditación de la primera tarjeta inteligente se da en el año de 1974, cuando Roland Moreno, un periodista francés, patentó la invención de una memoria electrónica montada en un anillo, la cual dio lugar a que en 1977 las empresas Bull y Motorola, crearan una tarjeta que tenía dos chips un microcontrolador y una memoria separada.

En 1980, la empresa Motorola introdujo la primera tarjeta inteligente con un solo microchip [33]. Así, con el desarrollo de la telemática [29] y la información de las transacciones interbancarias, el dinero logra viajar de manera instantánea por vía telefónica a una velocidad mayor, formando una red bancaria internacional de transferencias electrónicas donde es posible trasladar de país a país grandes cantidades de dinero electrónico en segundos. Dado que la seguridad social y el sistema federal de pensiones brindaron a sus clientes la posibilidad de depositar su dinero en cuentas bancarias, el sistema electrónico comenzó a popularizarse alrededor de 1971 junto con la invención del cajero automático [34].

Luego, en 1974 los comercios comenzaron a adquirir unos aparatos capaces de leer la banda magnética de las tarjetas de crédito y registraban el pago realizado a determinado negocio en la cuenta bancaria del propietario por medio de la red de telefonía, así las compras cotidianas entraron a formar parte de las transacciones electrónicas [10]. Para 1995 cerca del 90% de las transacciones en Estados Unidos eran hechas electrónicamente [34], mientras que para 1998, cerca del 84% de la población adulta del Reino Unido poseía algún tipo de tarjeta de pago de plástico [31].

Desde allí se empieza a crear el dinero electrónico, que es definido como el conjunto de medios de pago que requiere para su funcionamiento mecanismos electrónicos (tarjetas de crédito, débito, inteligentes, monederos electrónicos, títulos electrónicos como cheques y letras de cambio, cartas de crédito electrónicas, y otros pagos B2B). Estos pueden tener efectos sobre la oferta de dinero y manejo de la política monetaria por parte de las autoridades [10], [35]. El mismo es almacenado en un soporte electrónico, emitido al recibir fondos de un importe no inferior en valor que el valor monetario emitido y aceptado como medio de pago por empresas distintas del emisor [36]. Sin embargo,

para aumentar la confianza de los consumidores los pagos electrónicos deben considerar algunas condiciones [37], [38]. Como lo menciona Weatherford, hoy en día el dinero electrónico se está convirtiendo en una amenaza para muchos [18].

En los últimos años, con la llegada y penetración del internet se ha evidenciado el crecimiento de comunidades virtuales, las cuales en ocasiones han creado y distribuido su propia moneda virtual para el intercambio de bienes y servicios. Banesto fue la institución española pionera en lanzar al mercado la primera tarjeta virtual denominada Virtual Cash [10]. Son muchas las monedas virtuales que son utilizadas con mayor o menor éxito en la red: desde Pecunix [39], hasta Liberty Reserve y e-gold (las dos últimas fueron cerradas por el gobierno de Estados Unidos por sus operaciones ilegales en las transacciones), así como las asociadas al ocio como Linden Dollars de Second Life [40] o Facebook Credits [41] de Facebook [42].

De esta manera, la moneda virtual es un tipo de dinero digital no regulado que se caracteriza por actuar como medio de intercambio y como unidad de cuenta dentro de una comunidad virtual en particular, la cual es emitida y controlada por sus creadores. Puede tener aspectos positivos si contribuyen a la innovación financiera y ofrecer alternativas de pago adicionales a los consumidores, y de igual manera presentar riesgos para sus usuarios debido a la falta de regulación [43], [44]. Es así como a lo largo de la historia se han evidenciado diferentes formas de concebir el dinero para facilitar el comercio, comenzando por el trueque con el cual se utilizaron muchos tipos de bienes como medios generales de pago, hasta que finalmente se llega al dinero digital que es la forma de dinero más reciente. Entonces se puede deducir que la aparición del dinero virtual es un desarrollo de las formas de dinero anteriormente mencionadas como se puede observar en la figura 1 [43], [45]:

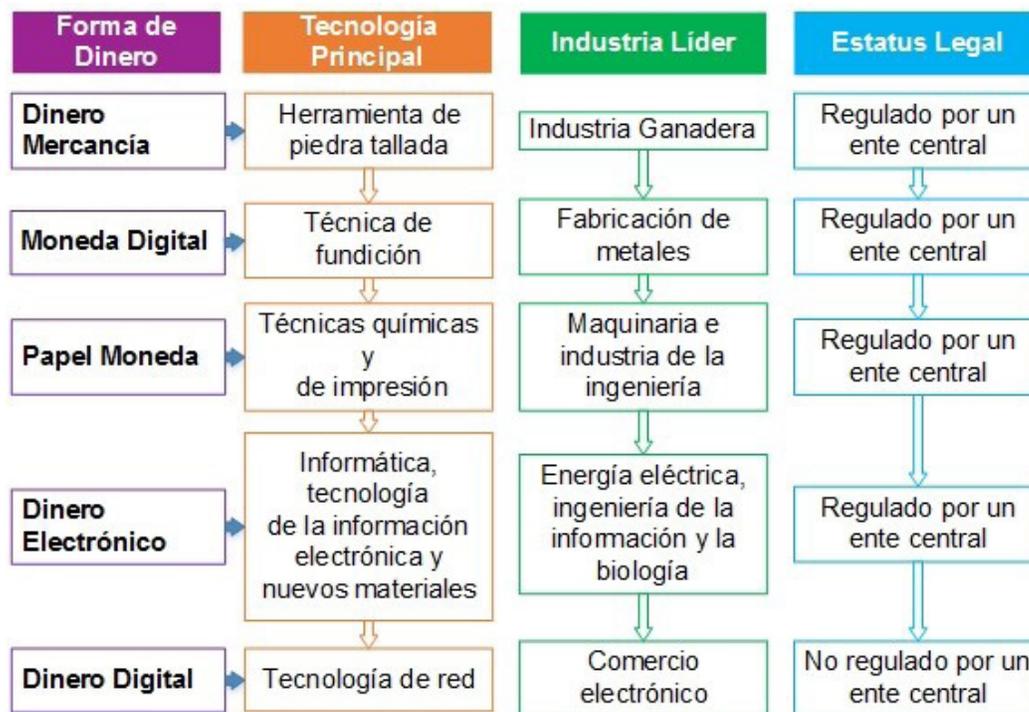


Figura 1. Desarrollo de las formas de dinero.

Yankee Group pone de manifiesto que el mercado de las divisas virtuales en el 2012 tenía un valor de USD\$ 47,5 mil millones y se proyecta que crezca un 14 % durante los próximos cinco años, llegando a USD\$ 55,4 billones en 2017 [46]. Como se observa en la figura 2, las monedas virtuales maduras comprenden el 95 %, captando la mayor parte del mercado, y se puede predecir que a medida que estas tendencias evolucionen las monedas digitales ganarán mayor aceptación frente a las monedas tradicionales.

2. BITCOIN

El Bitcoin es definido como una fuente abierta de dinero electrónico y pagos en la red que actúa como moneda alternativa, moneda digital o criptomoneda virtual. Esta moneda usa algoritmos criptográficos para garantizar las transacciones y es certificada por una red de usuarios en lugar de un banco central o sistema de reserva fraccionaria que controle su suministro, a diferencia del dólar, euro,

yen o cualquier otra moneda física tradicional. Asimismo, permite ejecutar transacciones totalmente públicas a través de un sistema peer to peer de pago y consultar cualquier movimiento realizado desde que inició hasta la actualidad [47]-[53].

Al tomar como referencia las tres funciones de la moneda tradicional dentro de la economía (medio de cambio, acumulación de valor, unidad de cuenta) y relacionarlas con el Bitcoin se evidencia que: como medio de cambio, funciona como una red de intercambio entre pares, asimismo satisface la coincidencia de necesidades recíprocas, aunque carece de liquidez porque no ha sido totalmente aceptada; como acumulación de valor, su gran volatilidad hace que sea difícil de predecir y por tanto puede resultar un instrumento arriesgado para almacenar valor y como unidad de cuenta, todavía está restringida a un pequeño grupo de empresas e individuos[54], [55]. En la Tabla 1 se evidencian las generalidades del Bitcoin.

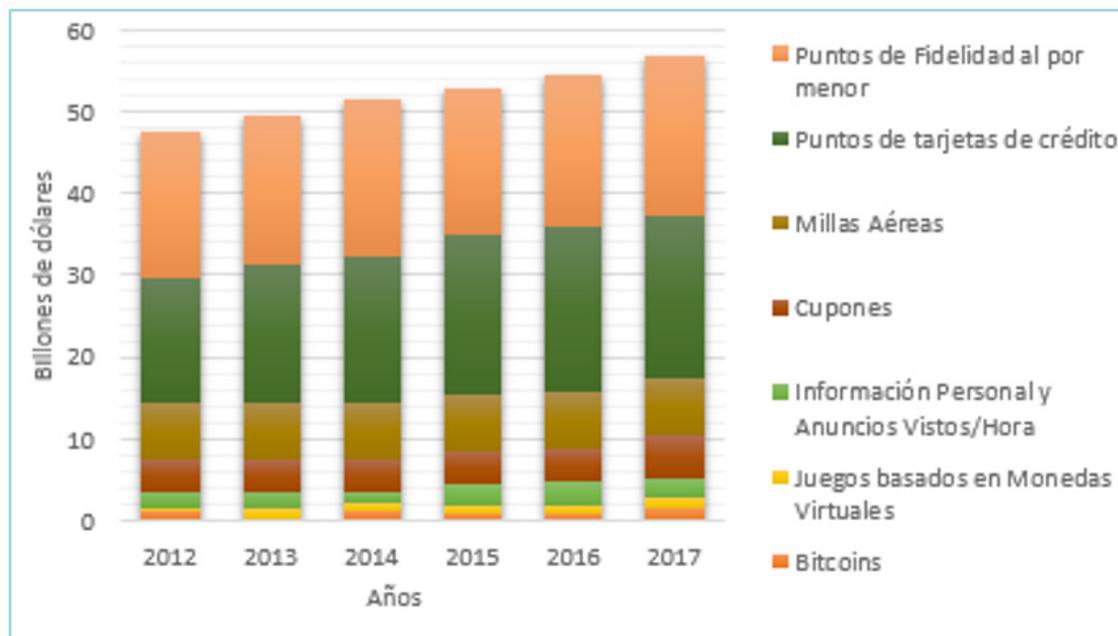


Figura 2. Cinco años de crecimiento del mercado de las monedas virtuales. **Fuente:** adaptado de Yankee Group [46].

Tabla 1. Generalidades del Bitcoin.

| Parámetro | Descripción |
|-----------------------------------|---|
| Símbolo | Se usa informalmente BTC, otros usan XBT. |
| Denotación | Bitcoin: se refiere al sistema de pago. bitcoin : unidad de cuenta del sistema de pago. |
| Divisibilidad del bitcoin | Un bitcoin se subdivide en 100 millones de unidades más pequeñas llamadas satoshis, fraccionada hasta 8 decimales [56]. |
| Cierre más alto del precio | Nov 25, 2013 USD\$ 1.119 [57]. |
| Cierre más bajo del precio | Abril 23,2012 USD\$ 4,91 [57]. |
| Startups* de Intercambio | Bitstamp [58] (sirve a la industria Bitcoin desde el 2011, primer plataforma en dólares), Btc-e [59], Bitfinex [60], Kraken [61] (primer plataforma en euros), LocalBitcoins [62] (entre individuos). |
| Startups que aceptan bitcoins | Bitpay [63] (el proveedor más grande de servicios de pago, usado por Microsoft y Wordpress), Coinbase [64] (servicio todo en uno: billetera y pagos, usado por Dell y Expedia). |
| Sitios de información | Bitcoin.org [65] (sitio completo manejado por la comunidad), Bitcoin Wiki [66] (Wiki acerca de Bitcoin), BitcoinTalk [67] (Primer foro dedicado a Bitcoin), Blockchain.info [68] (Explorador de bloques Bitcoin). |
| Cajeros automáticos Bitcoin (ATM) | Los primeros lugares en tener ATM fueron Carolina del Sur [69], San Francisco, Tokyo, Singapore [70], London [71], Tucson y Canadá [72]. El primer ATM del mundo abrió sus puertas en Vancouver en octubre de 2013 y ofrece la conversión Bitcoin a dólares canadienses [73]. |

*Una compañía startup es un negocio con una historia de funcionamiento limitado. Generalmente son empresas asociadas a la innovación, al desarrollo de tecnologías, al diseño web o desarrollo web; son empresas de capital-riesgo.

3. DESCRIPCIÓN DEL PROTOCOLO BITCOIN

Esta moneda se anunció por primera vez el 1 de noviembre de 2008 mediante el paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [74], cuyo autor es Satoshi Nakamoto (un programador pseudónimo probablemente) quien describió al Bitcoin como "un sistema para las transacciones electrónicas, sin depender de la confianza, a través del uso de la prueba criptográfica" [75]. El primer bloque creado (las primeras monedas que aparecieron en la red), denominado (bloque génesis) cuya recompensa por su solución fue de 50 bitcoins, empezó a funcionar el 3 de enero de 2009 [84], y el proyecto fue anunciado en la lista de correo Criptografía [163] el 11 de enero de 2009. Unos dieciocho

intercambios Bitcoin existen, ofreciendo servicios de cambio con muchas monedas en el mundo, (por ejemplo, EUR, USD, CAD, GBP, PLN, JPY, HKD, SEK, AUD, CHF, etcétera) [76].

Rice evidencia que el 6 de noviembre de 2013, el Wall Street Journal informó que la velocidad de la minería bitcoin era ahora 40 veces más rápida que en enero de 2013. Asimismo, que en los primeros cinco años se crearon 10,5 millones de bitcoins, para agosto del 2013 había en existencia 11,5 millones de bitcoins y se estima que el 90 % del límite de 21 millones de bitcoins se habrá producido en 2020, llegando así al límite de su oferta en el 2040 [77]. En la figura 3 se presenta el protocolo Bitcoin y el proceso de transar bitcoin [77]-[84]:

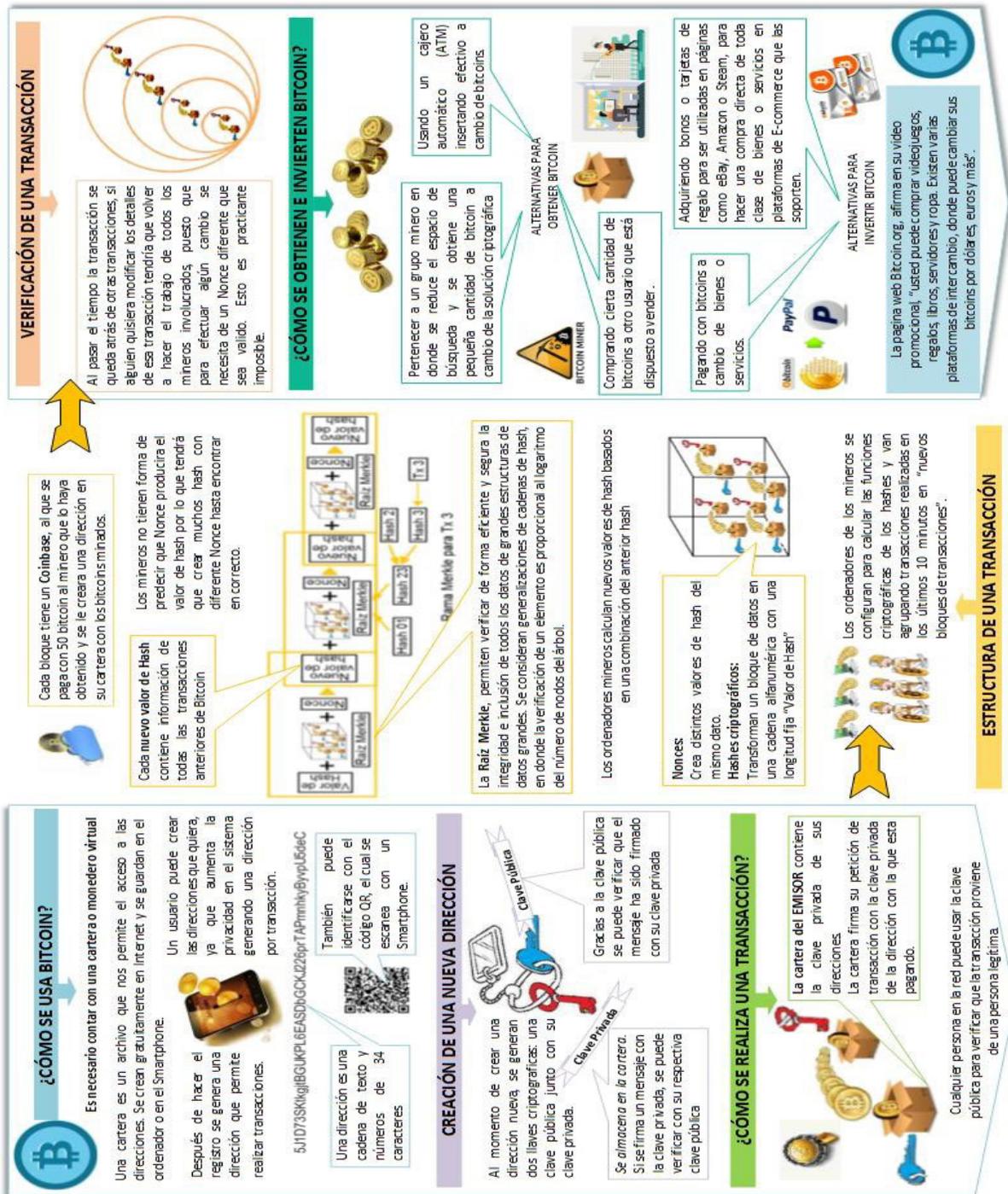


Figura 3. Generalidades del Protocolo Bitcoin y proceso de transacción.

4. FUNCIONAMIENTO DEL BITCOIN

Para que los usuarios puedan realizar transacciones de bitcoins, deben instalar una billetera digital en su ordenador o Smartphone. Una billetera es un archivo que contiene un número determinado de pares de claves criptográficas enlazadas a sus respectivas direcciones [85]. Bitcoin se basa en la criptografía de una clave pública y una privada: la clave pública está disponible para que cualquier usuario en la red la pueda ver, mientras que la clave privada es conocida solo por sus equipos [86]. Los usuarios que reciben bitcoins envían sus claves públicas a los usuarios para transferir los bitcoins y quienes transfieren las monedas firman con sus claves privadas, y la transacción se transmite entonces por la red Bitcoin [87]. Los bitcoins se envían y reciben a través de direcciones, que son largas secuencias alfanuméricas entendidas por la red. Para el envío de bitcoins, simplemente se introduce la dirección del receptor en la billetera, en otros casos esta dirección se codifica como código QR [88].

Cuando cierta cantidad de bitcoins se envían de una billetera a otra la transacción es recogida por la red, sin embargo la transacción debe ser verificada. Los mineros convierten la información del bloque en una secuencia alfanumérica, que de manera efectiva produce una firma y un sello de tiempo usando una función criptográfica. Esto se conoce como el Hash (en el caso de Bitcoin, es Secure Hash Algorithm SHA-256), esta firma evita que la transacción sea alterada por alguien, una vez que se ha emitido [89], [90]. Por lo anterior, el Bitcoin tiene como característica el anonimato, esto significa que un usuario es anónimo con respecto a un conjunto de usuarios [91],[92]. Por otro lado, se evidencian intentos para poder obtener la identificación de los usuarios Bitcoin [79], [93]. Juskalian relata cómo sería vivir durante 48 horas solo con transacciones en bitcoins [94].

4.1. La minería Bitcoin

Al momento de efectuar una transacción se genera un cambio de propiedad, donde no se puede verificar si uno de los dueños hizo un doble gasto de la moneda [95], [96]. La solución es estar al tanto de todas las transacciones (para lograrlo sin intermediarios se deben hacer públicamente), contando con usuarios que estén de acuerdo con un historial de marcas de tiempo. Cuando se realiza una transacción cada usuario puede tener certeza de que la mayoría de los nodos estuvieron de acuerdo con ese cambio de propiedad, ya que todas las transacciones son difundidas entre los usuarios mediante un libro de contabilidad pública, que sirve como soporte de la red Bitcoin y permite registrar todas las transacciones que por lo general comienzan a ser confirmadas por la red en los siguientes diez minutos [97].

Cada transacción se envía a un bloque que posteriormente se agrupa en una cadena de bloques, mediante un proceso que implica el cálculo repetido de una función hash [98]. Cada bloque de hash es único y se genera, en parte, utilizando el hash del bloque anterior. De esta manera, la billetera calcula el saldo gastable y las nuevas transacciones pueden ser verificadas. A través de una prueba de cifrado, se verifica y recopila la transacción a lo largo de otras transacciones pendientes, y una vez arbitraria esta tiene una forma específica; es así como se descentraliza la verificación y el registro de transacciones [75], [99].

Para la solución exitosa de este laberinto criptográfico conocido como minería, el proceso requiere un considerable esfuerzo y equipo computacional que es recompensado con bitcoins recién generados y/o comisiones de movimiento, esta recompensa es actualmente de 25 bitcoins por bloque, pero se reducirá a 12,5 bitcoins por bloque alrededor del año 2017 [100]. Una vez los bitcoins se extraen

con éxito, se genera la clave privada oculta que se utiliza para firmar transacciones y permite el acceso a los bitcoins (si esta se pierde, los bitcoins se han ido para siempre). Como lo dan a conocer O'Dwyer y Malone, en la figura 4 se aprecia la dificultad de encontrar un nuevo bloque con el paso del tiempo [101].

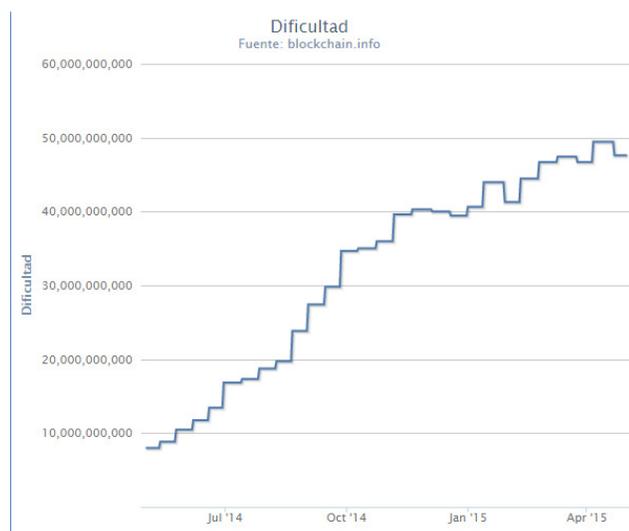


Figura 4. Dificultad para generar nuevos bloques.
Fuente: Blockchain.info [102].

En sus inicios, un bitcoin se compraba por 25 centavos en un intercambio, y un minero con solo la CPU de un ordenador podía minar una cantidad considerable de nuevos bitcoins en un día. Con el paso del tiempo la creación de bitcoins ha aumentado su complejidad [103], lo que significa que los mineros necesitan constantemente la potencia de procesamiento más avanzada para competir, siendo indispensable las computadoras diseñadas exclusivamente para la minería. Como consecuencia han surgido las siguientes tecnologías para hacer minería, cada una de ellas más rápida y eficiente que la anterior: CPU, GPU, FPGA y la que actualmente se utiliza: la plataforma de circuito integrado de aplicación específica (ASIC), diseñada particularmente

para ejecutar la operación de hash [104]. De este modo, Taylor describe en detalle la evolución de los hardware anteriormente mencionados para la minería Bitcoin [105].

4.2. Prueba de trabajo

Bitcoin hace que sea computacionalmente difícil trabajar un bloque, al exigir que el hash resultante tenga propiedades numéricas específicas. Lo anterior conlleva a un complejo trabajo por parte de los mineros, ya que es necesario mantener un registro de identificación de la cadena de bloques mediante una prueba-de-trabajo [106]. Este se logra estando seguro de tener la cadena más larga con el fin de obtener la rama de Merkle (la cual enlaza la transacción al bloque en que ha sido fechado) [107]. Para el cálculo de la función hash se combinan datos de bloques anteriores y un nonce [108]. El "nonce" de un bloque Bitcoin es un campo de 32 bits (4 bytes) cuyo valor se establece de modo que el hash del bloque contenga una cadena de ceros para controlar la complejidad en los cálculos de los nuevos bloques [109]. A fin de encontrar un bloque válido la única alternativa será ir obteniendo diferentes nonce hasta encontrar uno que cumpla el requisito preestablecido [110], dado que las funciones hash criptográficas no son invertibles.

4.3. El proceso de transacción Bitcoin

La base de Bitcoin son dos esquemas criptográficos: la firma digital y el hash criptográfico.

- **Firma digital:** permite el intercambio de instrucciones precisas de pago entre cada una de las partes de la transacción. Esta sirve para formalizar un mensaje entre el emisor y el receptor asegurando: autenticación (el receptor verifica que el mensaje proviene del emisor), no abandono (el emisor no puede rechazar el envío del mensaje), e integridad (el mensaje no puede ser manipulado). El hash se entrega con

la clave privada, y el resultado será la firma digital. Luego, el documento se entrega junto con la firma digital y la clave pública. Al final del proceso de verificación si los hashes coinciden la firma es válida. En la figura 5 se presenta el proceso de firma digital en un mensaje [111]:

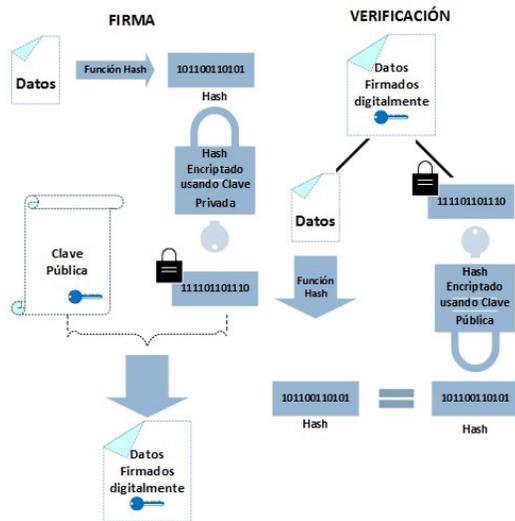


Figura 5. Proceso de firma digital de un mensaje.

- **Hashes criptográficos:** es un algoritmo que toma como entrada unos datos de longitud cualquiera (mensaje) y devuelve una cadena de

bits de longitud fija (hash). Las funciones hash aseguran: resistencia a preimagen, resistencia a segunda preimagen y resistencia a colisión [111].

5. VOLATILIDAD, RIESGOS Y ATAQUES QUE HA SUFRIDO EL BITCOIN

A pesar de que Bitcoin no tiene un valor intrínseco, su precio ha sido muy volátil, este se ha elevado hasta alcanzar máximos y luego ha bajado rápidamente hasta llegar a valer casi nada. Por ejemplo, en enero de 2013, un bitcoin fue cambiado por USD\$ 20; el 10 de abril, el tipo de cambio alcanzó USD\$ 266 dólares y después de tres días se redujo a USD\$ 54 [112]. En diciembre de 2013, el valor de mercado de un bitcoin disparó más allá de USD\$ 1000 y alcanzó un récord de USD\$ 1242, a principios de 2014 este bajó y llegó a valer USD\$ 900 [113]. Por otra parte, los precios de Bitcoin han demostrado históricamente ser muy sensibles a los acontecimientos referentes al sistema de pago. Por ejemplo, el precio Bitcoin cayó más o menos un 18 % el 2 de octubre de 2013, el día de los arrestos de la Ruta de la Seda. Al día siguiente los precios subieron un 13,9 % [114]. En la figura 6 se muestra el precio del mercado de bitcoins en el último año.

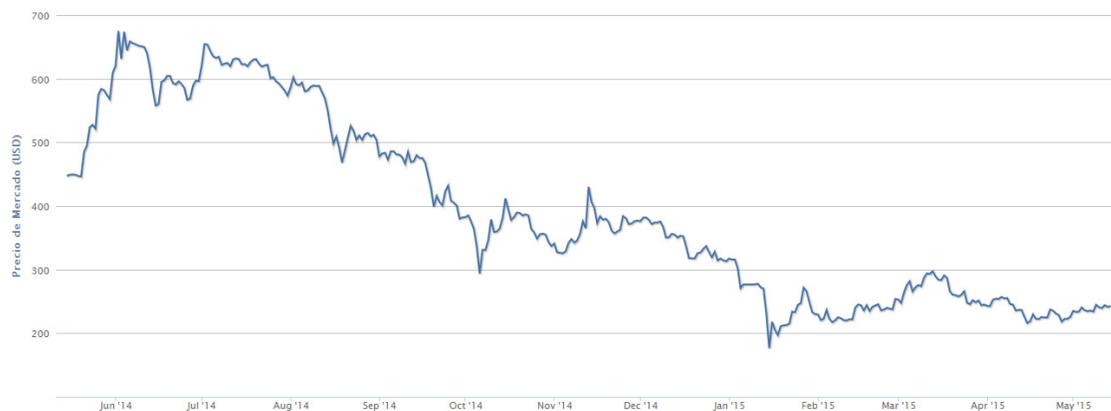


Figura 6. Precio del Mercado de bitcoins en Dólares. Fuente: Blockchain.info [102].

Según Blockchain.info, a la fecha de 25 de abril de 2015 el valor de bitcoin en el mercado se encontraba alrededor de \$226,88 USD (ponderado). Algunas personas tienen la expectativa de que gracias a la volatilidad pueden obtener grandes cantidades de dinero rápidamente, pero también se puede perder en un momento. Wu y Pandey mencionan casos en que los usuarios se han enriquecido y otros que han quedado en la ruina por la pérdida de grandes cantidades de bitcoin, debido a la variación en su precio [115]. Es sabido que la volatilidad del Bitcoin es mayor que la del dólar estadounidense [116]. Doug asegura que hasta el 2014 este mercado era muy pequeño comparado con el dólar: el valor de todos los bitcoins en circulación era USD\$ 5900 millones, un 0,05 % el tamaño del dinero de EE.UU [117].

En CRIMA Portfolio, se afirma que la oferta limitada de bitcoins hace que los precios suban y fluctúen debido a la especulación, y a menos que los precios se estabilicen, invertir en la moneda virtual es una gran apuesta [118]. La figura 7 da a conocer eventos importantes sobre la volatilidad que ha sufrido la moneda desde el inicio de sus operaciones y casos donde el Bitcoin ha sido objeto de ataques desde múltiples direcciones, incluyendo robos masivos, fraudes y actividades criminales, así como posibles ataques que involucran transacciones polvo y de doble gasto [119]-[134].

6. VENTAJAS Y DESVENTAJAS DEL BITCOIN

6.1. Ventajas

Algunas ventajas del Bitcoin destacadas por Vásquez son: la moneda no es embargable, se pueden tener varias cuentas pudiendo ser diversificadas en distintos lugares del mundo, no es necesario la tutela de un gobierno a través de instancias de política monetaria, funciona sin interrupciones las 24 horas del día, no tiene intermediarios para realizar un cobro o un pago, tiene costos bajos por administraciones de

gestión en internet y permite almacenar importantes sumas de dinero equivalentes en bitcoins y sin costo extra de administración [123].

Por otra parte, el Bitcoin omite por completo el sistema tradicional, ya que las transacciones se hacen *peer to peer* como dinero digital y su irreversibilidad elimina la posibilidad de fraude (lo que permite a los comerciantes aceptar pagos con confianza y mantener tasas bajas, contrario a las empresas que trabajan con tarjeta de crédito las cuales exigen una cuota alrededor del 3 % en cada compra), proporcionando altos niveles de anonimato de los remitentes y receptores [135]-[139].

Asimismo, Bitcoin permite su intercambio por monedas tradicionales en muchas casas de cambio a través de diversos intermediarios, e incluso a través de los cajeros automáticos. Hay quienes en Silicon Valley creen que Bitcoin podría reemplazar las monedas fuertes tradicionales, especialmente en países con altas tasas de inflación [140] y [141].

6.2. Desventajas

Como desventajas del Bitcoin se consideran: la incertidumbre, la falta de regulación y las externalidades de la red. Asimismo, el Bitcoin al ser un sistema descentralizado tiene el potencial de amenazar la estabilidad económica mundial por la que el FMI fue creado para proteger [142]. Igualmente, una eventual colocación del Bitcoin puede afectar la estabilidad financiera [143]. Aunque Bitcoin proporciona características que aumentan la privacidad de las transacciones, al mismo tiempo estas pueden ser usadas por usuarios malintencionados para ejecutar robos y acciones delictivas. Por ejemplo, gracias al anonimato y a la dificultad para enlazar las transacciones con sus respectivos emisores, Bitcoin puede ser usado para lavar dinero, para comercio ilícito y para el tráfico de sustancias y productos ilegales (drogas, armas), o para financiación de organizaciones criminales [144].

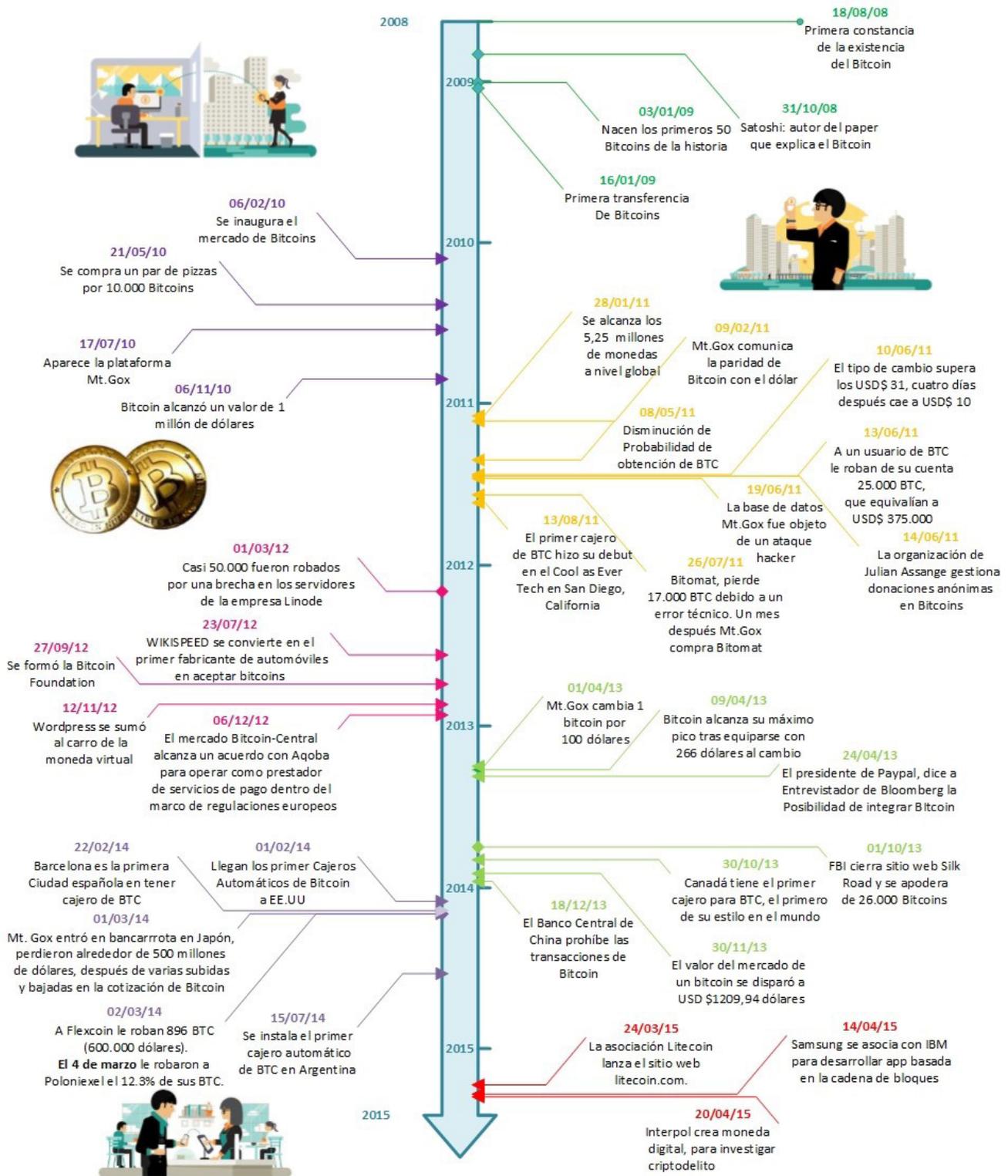


Figura 7. Cronología del Bitcoin.

Se afirma que en principio el suministro de bitcoins podría ser lo suficientemente sólido para funcionar como un sustituto de la moneda, pero aún no está listo para desempeñar este papel. Asimismo, asegura que su tecnología es más como Windows, iOS o Android en sus primeras etapas, por lo que necesita un ecosistema de productos y servicios complementarios para hacer esta tecnología fácil de utilizar [145]. Hasta que la moneda no se estabilice y existan métodos fiables para el seguimiento de su uso, Bitcoin podría presentar dificultades reales de contabilidad y preservación de capital en las industrias. Por ejemplo, hay casos donde el Bitcoin ha llevado a compañías a la quiebra, como es el caso de Alydian [146].

7. RECONOCIMIENTO Y ACEPTACIÓN DEL BITCOIN POR ORGANISMOS INTERNACIONALES

Algunos comerciantes conocidos a nivel internacional, tales como la compañía de computadores Dell (en julio de 2014 anunció que aceptaría

bitcoins como el pago a través de su sitio web) [147], Expedia, y Overstock.com se unieron a la red Bitcoin, junto con una serie de empresas más pequeñas, como el Tea Company Nuevo México y la colina de césped Alpacas. Incluso el United Way ahora acepta donaciones en bitcoin [104]. Ah Kun muestra algunos ejemplos de compañías que también aceptan bitcoins [148].

La complejidad de la implementación de un marco regulatorio se enfatiza en aspectos jurídicos importantes como la protección de datos y privacidad, la protección del consumidor, las cuestiones de derecho internacional privado, la legislación del comercio electrónico incluyendo cuestiones de responsabilidad en mundos virtuales, los aspectos de regulación financiera y el conocimiento del cliente [149]. Aun así, hay países que han empezado a definir y aplicar un marco regulatorio para el Bitcoin gracias a la popularidad que ha tenido en los mercados internacionales [57],[150]-[157], como se evidencia en la figura 8.

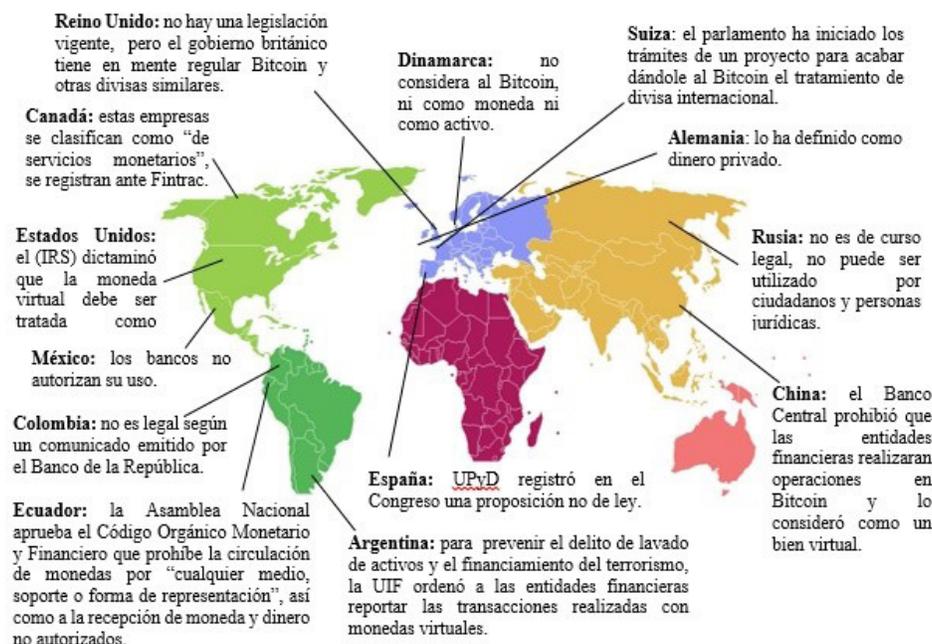


Figura 8. Reconocimiento del Bitcoin por organismos internacionales.

Se podría argumentar que Bitcoin y otras monedas digitales se encuentran en algún lugar de la frontera entre divisas, materias primas y activo financiero, o simplemente no existe regulación alguna por la confusión en su tratamiento fiscal [158]-[160]. Existen páginas donde se pueden consultar eventos, conferencias y reuniones a realizar alrededor de los mundos programados para el presente año, relacionados con el Bitcoin [161], [162].

8. CONCLUSIÓN Y ESTUDIOS FUTUROS

Con la invención del Bitcoin se rompe el paradigma en el que se entiende el dinero, como sucedió con la invención de la imprenta pasando del intercambio con monedas al intercambio con billetes. Las diferentes formas que el dinero ha adoptado a lo largo de la historia han venido acompañadas de una reducción en los costos de transacción, y Bitcoin no es la excepción. Este sistema es considerado como un mecanismo de intercambio al contar con las características de una moneda virtual, ganando mayor popularidad al ser aceptada en más lugares como medio de pago, al igual abre la posibilidad de ser una nueva forma de realizar transacciones: haciendo posible negocios de forma dinámica. Para unos cuantos, Bitcoin es tan solo una burbuja económica que tarde o temprano terminará explotando, pero para otros podría ser la moneda que cambiará al mundo en cuanto a los pagos online, esto no es del todo inverosímil ya que se cuenta con la tecnología, y se está pensando en la necesidad de infraestructura para que este sistema sea reconocido como una forma de intercambio comercial aceptado y respaldado mundialmente. Algunos países han propuesto su regulación aumentando el control por parte de autoridades, ya que los servicios financieros podrían ser potencialmente alterados. Otros no se han pronunciado al respecto, pero tampoco lo prohíben.

Hay oportunidades para las grandes empresas de tecnología, quienes tienen la posibilidad de desarrollar la capacidad de procesamiento y convertirse

en cámaras de compensación de monedas digitales por sí mismas o a través de sociedades mixtas con entidades financieras. Pero aun así, existen varios aspectos sobre el sistema Bitcoin donde no se tiene claridad, como la contabilidad empresarial, la declaración de impuestos, el marco regulatorio y la seguridad en las transacciones (reducir la capacidad para falsificar una moneda fuerte). Si se pretende masificar la confianza del usuario, es necesario fortalecer el sistema en estos aspectos para que aun más empresas del sector tecnológico o startups le empiecen a apostar. Por lo tanto, las instituciones y reguladores financieros que entiendan y adopten finalmente el Bitcoin, tendrán más posibilidades de liderar el nuevo sistema monetario digital. Empresas del sector tecnológico o startups ya le están apostando al Bitcoin, como es el caso de la multinacional IBM que ha empezado a utilizar esta moneda para temas de Big data e internet de las cosas.

9. REFERENCIAS

- [1] "World Internet Usage and Population Statics", Internet World Stats-Usage and Population Statics, 2014, [en línea]. Consultado el 8 de abril de 2015, disponible en <http://www.internetworldstats.com/stats.html>
- [2] N. Safa and M. Ismail, "A customer loyalty formation model in electronic commerce", *Economic Modelling*, vol. 35, pp. 559-564, 2013.
- [3] Biblioteca Virtual Luis Ángel Arango, "Las tarjetas como dinero", [en línea]. Consultado el 29 de abril de 2015, Disponible en: <http://www.banrepcultural.org/blaavirtual/ayudade-tareas/economia/econo32.htm>
- [4] E. Cuervo, "Implementación de un monedero digital móvil", México, Centro de Investigación y de estudios avanzados del Instituto Politécnico Nacional, 2005.
- [5] M. Reina, S. Zuluaga y M. Rozo, *El dinero y la política monetaria*, Bogotá D.C, Banco de la República, Departamento de Comunicación Institucional, 2006.

- [6] M. Santana, "Reinventando el dinero. Experiencias con monedas comunitarias", México, Centro de Investigaciones y Estudios Superiores en Antropología Social, 2008.
- [7] J. Surowiecki, "A brief history of money", *IEEE Spectrum*, vol. 49, no. 6, pp. 44-79, 2012.
- [8] R. Bustamante, K. Escoto de Chávez, E. García y E. Turcio, "Evaluación de la moneda alternativa como un medio que posibilita la economía solidaria: caso de estudio Suchitoto", San Salvador, Universidad Centroamericana "José Simeón Cañas", 2012.
- [9] J. William y C. Eagleton, *Historia del dinero*, Barcelona, Paidós, 2009.
- [10] A. Gómez, "El dinero electrónico como sustituto parcial del efectivo y posible mecanismo para masificar el acceso a los servicios financieros. Análisis de la normativa costarricense y la comparada", Universidad de Costa Rica, 2012.
- [11] L. Aranda, "El uso de cacao como moneda en la época prehispánica y supervivencia en la época colonial", en XIII Congreso Internacional de Numismática, vol. 2, pp. 1439-1450, 2003.
- [12] K. Saito and E. Morino, "Towards Tangible 'Virtual Money'-Position Paper", in 6th IEEE Consumer Communications and Networking Conference, pp. 1-5, 2009.
- [13] L. Wray, "An irreverent overview of the history of money from the beginning of the beginning through to the present", *Journal of Post Keynesian Economics*, vol. 21, no. 4, pp. 679-687, 2015.
- [14] J. Hoyle and G. Whitehead, "The development of the money system", in *Elements of Banking. Made Simple Books*, William Heinemann, 1987, pp. 12-28.
- [15] A. Vico, "Monedas Griegas", Real Academia, Madrid, Real Academia de la Historia. *Catálogos del Gabinete de Antigüedades* II.2.1, 2006.
- [16] V. Godazgar and L. Haddadi, "The Mechanisms of the Bullion Markets and the Return of Gold (and Silver) as Money", in *7th International Conference on e-Commerce in Developing Countries: With Focus on e-Security*, 2013, pp. 1-14.
- [17] Instituto del Tercer Mundo (ITEM), Instituto de Estudios Políticos de América Latina y África, *Guía del Mundo 2008: el presente y sus razones*, SM 2007. 2008.
- [18] J. Weatherford, *The History of Money*, 1st Pbk. United States, The Crown Publishing Group, 2009.
- [19] D. Housel, *La historia del dinero*, Student, Huntington Beach, CA, Teacher Created Materials, Inc, 2008.
- [20] K. Reed, "The history of money: from cows to Bitcoin", *Tennessee Bar Journal*, vol. 50, no. 8, pp. 25-28, 2014.
- [21] R. Werner, "How do banks create money, and why can other firms not do the same? An explanation for the coexistence of lending and deposit-taking", *International Review of Financial Analysis*, vol. 36, pp. 71-77, 2014.
- [22] M. Gozalbes, *Historia del dinero*, Valencia, Museu de Prehistoria de Valencia, 2011.
- [23] A. Aparicio, "Historia económica mundial 1870-1950", *Economía Informa*, vol. 2013, no. 382, pp. 99-115.
- [24] M. Maggi y P. Parra, *¿Qué es un banco central?*, Bogotá D.C., Banco de la República.
- [25] E. Junguito y C. Ayala, "Autonomía del Banco de la República", Bogotá D.C., Pontificia Universidad Javeriana, 2000.
- [26] L. Rockwell, "Payment Cards", *Encyclopedia of Forensic Sciences*, vol. 2, pp. 432-438, 2013.
- [27] B. de España, "Clases de Tarjetas", [en línea]. Consultado el 23 de marzo del 2015, disponible en: <http://www.bde.es/clientebanca/productos/tarjetas/clases/clases.htm>
- [28] K. Carow and M. Staten, "Debit, credit, or cash: survey evidence on gasoline purchases", *Journal of Economics and Business*, vol. 51, no. 5, pp. 409-421, 1999.

- [29] "Is electronic money a disruptive technology?" *Card Technology Today*, vol. 12, pp. 12-14, 2000.
- [30] J. Weatherford, *La historia del dinero: de la piedra arsénica al ciberespacio*, Barcelona, Andrés Bello, 1997.
- [31] J. Rosario, "El dinero plástico", *Boletín del Instituto de Estudios Almerienses*, Instituto de Estudios Almerienses, pp. 193-214, 1992.
- [32] H. Ortiz, "Análisis de las Tarjetas de Crédito en Colombia", *Observatorio Económico de Santander*, Universidad Santo Tomás, p. 6, 2014.
- [33] K. Shelfer, C. Corum, J. Procaccino and J. Didier, "Smart Cards", *Advances in Computers*, vol. 60, pp. 147-192, 2004.
- [34] J. Aguirre, *Historia del dinero en el siglo XX*, México, 1997.
- [35] Subdirección General de Estudios del Sector Exterior, "Dinero e Internet", *Boletín Económico de ICE*, no. 2729, pp. 3-6, 2002.
- [36] J. Guo and A. Chow, "Virtual money systems: A phenomenal analysis", in *10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services*, 2008, pp. 267-272.
- [37] N. Waraporn, M. Sithiyavanich, H. Jiarawattanasawat and N. Pakchai, "Virtual Credit Cards on Mobile for M-Commerce Payment", in *IEEE International Conference on e-Business Engineering*, 2009, pp. 241-246.
- [38] H. Kinoshita, M. Kudo, T. Morizumi and K. Suzuki, "An Electronic Money System as Substitute for Banknotes", in *0th Annual International Symposium on Applications and the Internet*, 2010, pp. 316-319.
- [39] "Pecunix", [en línea]. Consultado el 8 de abril de 2015, disponible en: <http://www.pecunix.com/>
- [40] "Second Life", [en línea]. Consultado el 8 de abril de 2015, disponible en: <http://secondlife.com/>
- [41] "Facebook Came Cards", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://www.facebook.com/credits/>
- [42] F. Brezo, "Aplicaciones ciberdelictivas de criptomodivas como Bitcoin", Centro de Análisis y Prospectiva, Guardia Civil, España, 2012.
- [43] European Central Bank (ECB), "Virtual Currency Schemes", 2012.
- [44] S. Rotman, "El bitcoin versus el dinero electrónico", Washington D.C, Grupo Consultivo de Ayuda a los Pobres (CGAP), pp. 1-4, 2014.
- [45] L. Chen and H. Wu, "The influence of Virtual money to real currency: A case-based study", in *International Symposium on Information Engineering and Electronic Commerce*, 2009, pp. 686-690.
- [46] J. McKee, "Redefining Virtual Currency", *Yankee Group*, pp. 1-11, 2013.
- [47] S. Feld, M. Schönfeld and M. Werner, "Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective", in *The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014)*, 2014, vol. 32, pp. 1121-1126.
- [48] J. Connell, "Alderney: gambling, Bitcoin and the art of unorthodoxy", *Island Studies Journal*, vol. 9, no. 1, pp. 69-78, 2014.
- [49] V. Gonzales, "Análisis sobre el origen, comportamiento y crecimiento del mercado del Bitcoin", México, Colegio de Postgraduados-Institución de Enseñanza e Investigación en Ciencias Agrícolas, 2014.
- [50] A. Campos, "Estudio de la red Bitcoin", Cataluña, Universidad Oberta de Catalunya, 2013.
- [51] M. Sudacevski, "Bitcoin-Un Nou Tip de Moned", *Management Intercultural*, vol. 15, no. 3, pp. 340-348, 2013.
- [52] D. Yermack, "Is Bitcoin a Real Currency? An economic appraisal", *Working paper, NBER*, pp. 1-14, 2013.
- [53] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph", in *Financial Cryptography and Data Security. 17th International Conference, FC 2013*, 2013, no. 7859, pp. 6-24.

- [54] S. Lo and J. Wang, "Bitcoin as Money?", *Federal Reserve Bank of Boston*, vol. 14, no. 4, pp. 1-28.
- [55] N. Karp, M. Nava, B. Stacey, C. Cuesta, O. Gouvela and A. Neut, "Bitcoin: A Chapter in Digital Currency Adoption", United States, Spain, 2013.
- [56] R. Joseph Cook, "Bitcoins: Technological Innovation or Emerging Threat?", *The John Marshall Journal of Information Technology & Privacy Law*, vol. 30, no. 3, pp. 535-570, 2014.
- [57] A. Cofnas, "Bitcoin: Currency or Commodity?", *Futures: News, Analysis & Strategies for Futures, Options & Derivatives Traders*, vol. 43, no. 6, pp. 10-12, 2014.
- [58] "Bitstamp", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://www.bitstamp.net/>
- [59] "btc-e", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://btc-e.com/>
- [60] "Bitfinex", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://www.bitfinex.com/>
- [61] "Kraken", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://www.kraken.com/>
- [62] "LocalBitcoins", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://localbitcoins.com/fr/>
- [63] "Bitpay", [en línea], Consultado el 8 de abril de 2015, disponible en: <https://bitpay.com/>
- [64] "Coinbase", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://www.coinbase.com/>
- [65] "bitcoin.org", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://bitcoin.org/es/>
- [66] "Bitcoin Wiki", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://es.bitcoin.it/>
- [67] "BitcoinTalk", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://bitcoin-talk.org/>
- [68] "Blockchain.info", [en línea]. Consultado el 8 de abril de 2015, disponible en: <https://blockchain.info/es>
- [69] E. Nemeroff, "South Carolina Gets Its First Bitcoin ATM", *American Banker*, vol. 179, no. F315, United States, apr-2014.
- [70] Global News, "Bitcoin ATM set up in Singapore", *Global Banking News*, feb-2014.
- [71] PR Newswire, "My Wallet LTD Pioneers Bitcoin ATMs in Major European Capital Cities", *PR Newswire US* mar-2015.
- [72] P. Liljas, "World's First Bitcoin ATM Launched in Canada", *Time.com*, p. 1, oct-2013.
- [73] E. Cohen, "The Bitcoin Economy", *Business NH Magazine*, p. 2, 23-jul-2014.
- [74] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", pp. 1-9, 2008.
- [75] J. Bohr and M. Bashir, "Who Uses Bitcoin? An exploration of the Bitcoin community", in *Twelfth Annual Conference on Privacy, Security and Trust (PST)*, 2014, pp. 94-101.
- [76] S. Barber, X. Boyen, E. Shi and E. Uzun, "Bit-ter to Better-How to make Bitcoin a Better Currency", in *16th International Conference, FC 2012, Financial Cryptography and Data Security*, 2012, p. pp 399-414.
- [77] D. Rice, "The Past and Future of Bitcoins in Worldwide Commerce", *Business Law Today BLT*, pp. 1-4, 2013.
- [78] M. Peck, "The cryptoanarchists' answer to cash", *Spectrum, IEEE*, vol. 49, no. 6, pp. 50-56, 2012.
- [79] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names", *Internet Measurement Conference-IMC, '13*, vol. 38, no. 6, pp. 127-140, 2013.
- [80] N. Neslund, "648 K-Bit About Bitcoin", *Singidunum Journal of Applied Sciences*, pp. 1-7, 2014.
- [81] K. Hill, "Living on Bitcoin a Year Later: The All-Bitcoin Start-Up With No Bank Account", *Forbes*, pp. 6-6, dec-2014.

- [82] J. Aron, "Building on Bitcoin", *New Scientist Magazine*, vol. 221, no. 2955, pp. 19-20, aug-2014.
- [83] Instituto Nacional de Tecnologías de la Comunicación (INTECO), "Bitcoin: Una moneda criptográfica", 2014.
- [84] G. Karame, E. Androulaki and S. Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin", in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2012, pp. 1-17.
- [85] P. Šurda, "Economics of Bitcoin : is Bitcoin an alternative to at currencies and gold?", *Wirtschafts Universitat Wien, Vienna University of Economics and Business*, 2012.
- [86] J. Brito and A. Castillo, "Bitcoin: A Primer for Policymakers", *Policy*, vol. 29, no. 4, pp. 3-12, 2013.
- [87] E. Gregersen, "Bitcoin", *Encyclopedia Britannica*, apr-2014.
- [88] D. Bradbury, "Bitcoin Bet", *Backbone Magazine*, pp. 24-27, nov-2013.
- [89] I. Miers, C. Garman, M. Green and A. Rubin, "ZeroCoin: Anonymous distributed e-cash from bitcoin", in *Proceedings - IEEE Symposium on Security and Privacy*, 2013, pp. 397-411.
- [90] S. Mantilla, *Bitcoin : la otra cara de la moneda*, 1ra ed. Buenos Aires, Instituto de Estrategia Internacional, 2014.
- [91] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Version 0.25", in *Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability*, 2000, p. 43.
- [92] M. Möser, R. Böhme and D. Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem", in *Proceedings of the 2013 e-Crime Researches Summit*, 2013, pp. 1-14.
- [93] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", in *2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing*, 2011, pp. 1318-1326.
- [94] R. Juskalian, "A Weekend in Bitcoin City : Arnhem, the Netherlands", *MIT Technology Review*, vol. 118, no. 2, pp. 69-72, 2015.
- [95] C. Beer and B. Weber, "Bitcoin-The Promise and Limits of Private Innovation in Monetary and Payment Systems", *Monetary policy & the economy: quarterly review of economic policy*, no. 3, pp. 53-66, 2014.
- [96] T. Bamert, C. Decker, L. Elsen, R. Wattenhofert and S. Welten, "Have a Snack, Pay with Bitcoins", in *13-th IEEE Internacional Conference on Peer-to-Peer Computing*, 2013, pp. 1-5.
- [97] A. Vance and B. Stone, "Bitcoin Rush: it takes an army of believers to mine a virtual currency", *Bloomberg Businessweek*, no. 4362, pp. 46-51, 2014.
- [98] B. Bradbury, "In Blocks We Trust", *Engineering & Technology*, vol. 10, no. 2, pp. 68-71, 2015.
- [99] G. Dwyer, "The Economics of Bitcoin and Similar Private Digital Currencies", *Journal of Financial Stability*, vol. 17, no. Instead of the Fed: Past and Present Alternatives to the Federal Reserve System, pp. 81-91, 2014.
- [100] M. Hall, "Bitcoin: Change You Can Believe In?", *PC Magazine*, june, pp. 10-14, 2013.
- [101] K. Dwyer and D. Malone, "Bitcoin Mining and its Energy Footprint", in *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CI-ICT 2014). 25th IET*, 2013, pp. 280-285.
- [102] "Blockchain.info", [en línea]. Consultado el 20 de abril de 2015, disponible en: https://blockchain.info/es/charts/market-price?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address

- [103] "Video: the Rise and Rise of Bitcoin", *Teletrabaja*, 2014, [en línea]. Consultado el 24 de abril de 2015, disponible en: <https://www.youtube.com/watch?v=YqfwGnW4aH4>
- [104] S. T. Middlebrook, "Bitcoin for Merchants: Legal Considerations for Businesses Wishing to Accept Bitcoin as a Form of Payment", *Business Law Today (BLT)*, 2014.
- [105] M. B. Taylor, "Bitcoin and The Age of Bespoke Silicon", in *Proceedings of the 2013 International Conference on Compliers, Architectures and Synthesis for Embedded Systems (CASES)*, 2013, pp. 1-10.
- [106] D. Kondor, M. Pósfai, I. Csabai and G. Vattay, "Do the rich get richer? An empirical analysis of the Bitcoin transaction network", *PLoS ONE*, vol. 9, no. 2, pp. 11-10, 2014.
- [107] G. Chaudhary, "Bitcoin : A Step Ahead in Technology", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 10, pp. 752-757, 2014.
- [108] N. Roth, "An Architectural Assessment of Bitcoin: Using the Systems Modeling Language", *Procedia Computer Science*, vol. 44, pp. 527-536, 2015.
- [109] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network", *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013-Proceedings*, pp. 1-10, 2013.
- [110] N. Wenker, "On line Currencies, Real-World Chaos: The Struggle to Regulate the Rise of Bitcoin", *Texas Review of Law Politics*, vol. 19, no. 1, pp. 145-197, 2014.
- [111] A. Badev and M. Chen, "Bitcoin : Technical Background and Data Analysis", *Working Papers, U.S. Federal Reserve Board's Finance & Economic Discussion Series*, pp. 1-38, 2014.
- [112] A. Rogojanu and L. Badea, "The Issue of competing Currencies. Case Study-Bitcoin", *Theoretical and Applied Economics: GAER review*, vol. 21, no. 1, pp. 103-114, 2014.
- [113] N. Sharon and S. John, "What You Need to Know About Bitcoins", *Law Practice: The Business of Practicing Law*, vol. 40, no. 5, p. 4, sep-2014.
- [114] P. Martinson and C. Masterson, "Bitcoin and the Secured Lender", *Banking & Financial Services Policy Report*, vol. 33, no. 6, pp. 13-20, 2014.
- [115] C. Wu and V. Pandey, "The Value of Bitcoin in Enhancing the Efficiency of an Investor's Portfolio", *Journal of Financial Planning*, vol. 27, no. 9, pp. 44-52, 2014.
- [116] J. G. Haubrich and A. Orr, "Bitcoin versus the Dollar", *Federal Reserve Bank of Cleveland, Economic Trends*, pp. 2-4, aug-2014.
- [117] H. Doug, "The Bitcoin Fantasy", *The Nation*, vol. 298, no. 20, pp. 12-17, 2014.
- [118] CRIMA Portfolio, "Is Bitcoin the next Bubble?", *Consumer Reports Money Adviser*, vol. 11, no. 4, p. 11, apr-2014.
- [119] D. Bradbury, "The problem with Bitcoin", *Computer Fraud & Security*, vol. 23, no. 11, pp. 5-8, 2013.
- [120] Elsevier B.V., "Massive Bitcoin thefts and seizures leave many users nervous and poorer", *Computer Fraud & Security*, vol. 23, no. 12, p. 1,3, 2013.
- [121] F. Y. Rashid, "How Thieves Steal Your Bitcoins", *PC Magazine Digital Edition*, pp. 17-20, apr-2014.
- [122] A. Phelps and A. Watt, "I shop Online - recreationally! Internet anonymity and Silk Road enabling drug use in Australia", *Digital Investigation*, vol. 11, no. 4, pp. 261-272, 2014.
- [123] M. VásquezLeiva, "Bitcoin : ¿Moneda o burbuja ?" *Revista Chilena de Economía y Sociedad*, vol. 8, no. 1-2, pp. 52-61, 2014.
- [124] M. Tilves, "Barcelona, primera ciudad española en tener cajero de Bitcoins", *WsiliconWeek*, 2014, [en línea]. Consultado el 8 abril de 2015, disponible en: <http://goo.gl/iQwePS>

- [125] M. Tilves, "Bitcoin: Cronología de una moneda", *Wsilicon Week*, 2013, [en línea]. Consultado el 8 de abril de 2015, disponible en: <http://www.siliconweek.es/cloud/bitcoin-cronologia-de-una-moneda-galeria-35533>
- [126] C. Evans-Pughe, A. Novikov and V. Vitaliev, "To bit or not to bit", *Engineering & Technology*, vol. 9, no. 4, pp. 82-85, 2014.
- [127] "Bitcoin ATM en funcionamiento" *ElBitcoin.org*, 2011, [en línea]. Consultado el 8 de abril de 2015, disponible en: <http://elbitcoin.org/bitcoin-atm-en-funcionamiento/>
- [128] R. Jarvis, "Bitcoin ATMs come to USA", *USA Today*, p. 1, feb-2014.
- [129] Rosh, "Samsung se asocia con IBM para desarrollar app basada en la cadena de bloques", *ElBitcoin.org*, 2015, [en línea]. Consultado el 27 de febrero de 2015, disponible en: <http://elbitcoin.org/noticias-bitcoin-del-dia-14-abril-2015/>
- [130] Y. Bello Perez, "Interpol Creates Digital Currency to Study Crypto Crime" *coindesk.com*, 2015, [en línea]. Consultado el 23 de abril de 2015, disponible en: <http://www.coindesk.com/interpol-creates-digital-currency-study-crime>
- [131] D. Cordell, "Litecoin Association Takes Step Forward and Launches Litecoin.com", *Bitcoinist.net*, 2015, [en línea]. Consultado el 23 de abril de 2015, disponible en: <http://bitcoinist.net/litecoin-association-takes-step-forward-launches-litecoin-com/>
- [132] K. Hill, "Bitcoin's Incredible Year", *Forbes, United States. Internal Revenue Service*, p. 1, dec-2013.
- [133] T. Lloyd, "Cryptocurrency Bitcoin Still On Rocky Path", *Investors Business Daily*, p. 1, feb-2015.
- [134] L. Trautman, "Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?", *Richmond Journal of Law & Technology*, vol. 20, no. 4, pp. 1-108, 2007.
- [135] M. Kevin, "The other side of the Bitcoin", *Newsweek Global*, vol. 162, no. 12, pp. 1-4, mar-2014.
- [136] T. Moore, "The promise and perils of digital currencies", *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3-4, pp. 147-149, dec-2013.
- [137] N. Yahanpath, "Virtual Money Betting on Bitcoin" *University of Auckland Business Review*, vol. 17, no. 1, pp. 3-43, 2014.
- [138] M. Van Alstyne, "Why Bitcoin Has Value", *Communications of the ACM*, vol. 57, no. 5, pp. 30-32, 2014.
- [139] P. Santhana, "The Pros and Cons of Bitcoins", *Baseline Magazine*, p. 1, Sep-2014.
- [140] "Bitcoin ATM Map", *CoinDesk*, [en línea]. Consultado el 24 de abril de 2015, disponible, [en línea]. Consultado el 24 de abril de 2015, disponible en: <http://www.coindesk.com/bitcoin-atm-map/>
- [141] K. Hill, "Why Are People So Excited About A Bitcoin ATM?", *Forbes, Internal Revenue Service*, oct-2013.
- [142] N. Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF", *Chicago Journal of International Law*, vol. 14, pp. 377-407, 2013.
- [143] J. Gómez-González and J. Parra-Polanía, "Bitcoin: something seems to be 'fundamentally' wrong", *Banco de la República*, pp. 1-9, 2014.
- [144] J. B. Turpin, "Bitcoin : The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework", *Indiana Journal of Global Legal Studies*, vol. 21, no. 1, pp. 335-368, 2014.
- [145] M. Cusumano, "The Bitcoin ecosystem", *Communications of the ACM*, vol. 57, no. 10, pp. 22-24, 2014.
- [146] D. Kronenberg and D. Gwen, "Bitcoins in Bankruptcy-Trouble ahead for Investors and Bankruptcy Professionals?", *Pratt's Journal of Bankruptcy Law*, vol. 10, no. 2, pp. 11-121, 2014.

- [147] The Federal Reserve Bank of St. Louis: Central to America's Economy, "Bitcoin and Beyond", *Central Banker-Fall*, vol. 24, no. 1, pp. 5-7, 2014.
- [148] A. Ah Kun, "Bitcoin: the currency of the future?", *Chartered Accountants Journal*, vol. 93, no. 4, pp. 36-38, 2014.
- [149] E. Jacobs, "Bitcoin: A Bit Too Far?", *Journal of Internet Banking & Commerce (JIBC)*, vol. 16, no. 2, pp. 1-4, 2011.
- [150] A. Cofnas, "Trading bitcoin", *Futures: News, Analysis & Strategies for Futures, Options & Derivatives Traders*, vol. 43, no. 10, pp. 10-10, 2014.
- [151] A. Blundell-Wignall, "The Bitcoin Questio". *Currency versus Trust-less Transfer Technology*, no. 37. Paris, OECD iLibrary, 2014.
- [152] Congreso de los Diputados, Boletín Oficial de las Cortes Generales: Proposiciones No de Ley-BOCG-10-D-592. España, 2015, p. 24.
- [153] A. General, Código Orgánico Monetario y Financiero, Libro I. Of. No. SAN-2014-1305. Distrito Metropolitano de Quito, Provincia de Pichincha, 2014, pp. 1-181.
- [154] "China Bans Financial Companies From Bitcoin Transaction" Bloomberg Business, dec-2013.
- [155] Banco de la República, "Comunicado Bitcoin", Banco Central de Colombia, Bogotá D.C, 01-apr-2014.
- [156] C. Viegas y J. G. Santamaría, "Bitcoin: Un desafío para la ejecución de políticas de la Banca Central. Algunas consideraciones jurídicas frente al creciente fenómeno de las llamadas 'criptomonedas'", Banco Central de la República de Argentina. Buenos Aires, Argentina, pp. 1-51, 2014.
- [157] K. Hill, "China Bites Into Bitcoin", *Forbes*, vol. 193, no. 1, pp. 43-43, jan-2014.
- [158] J. Lee, A. Long, M. McRae, J. Steiner and S. Gosnell Handler, "Bitcoin Basics: a Primer on Virtual Currencies", *Business Law International*, vol. 16, no. 1, pp. 21-46, 2015.
- [159] S. N. Navarro, "Un Mercado Financiero Floreciente : El del dinero virtual no Regulado", *Revista CESCO de Derecho de Consumo*, vol. 13, pp. 79-115, 2015.
- [160] C. Raibom and M. Sivitanides, "Accounting Issues Related to Bitcoins", *The Journal of Corporate Accounting & Finance*, pp. 25-34, 2015.
- [161] Bitcoin.org, "Conferencias y eventos", [en línea]. Consultado el 23 de abril de 2015, disponible en: <https://bitcoin.org/es/eventos>
- [162] Inside Bitcoins, "Upcoming Shows", [en línea]. Consultado el 23 de abril de 2015, disponible en: <http://insidebitcoins.com/upcoming-shows>
- [163] Bitcoin P2P e-cash paper, 2008, [en línea]. Consultado el 23 de abril de 2015, disponible en: <https://www.mail-archive.com/cryptography@metzdowd.com/msg099599.html>

