Universidad de Valladolid

Facultad de Ciencias Económicas y Empresariales

Trabajo de Fin de Grado

Grado en Finanzas Banca y Seguros

CRIPTOMONEDAS

Presentado por:

Zulema Figuero Castilla

Tutelado por:

María Dolores Soto Torres

Valladolid, 17 de Julio de 2020

ÍNDICE

RESUMEN

El objetivo de este trabajo es analizar distintos aspectos ligados al fenómeno de las criptomonedas: qué son, cómo se crearon, cómo funcionan, qué pretenden, cuántas hay, quién las crea o qué ventajas ofrecen, son algunas de las preguntas que este trabajo pretende contestar. Para abordar todos estos aspectos, el trabajo comienza repasando cómo se han ido modificando los medios de pago, la evolución de la tecnología y el desarrollo de la filosofía que sustentó la creación de la primera criptomoneda, el bitcoin. El trabajo continúa analizando cómo opera el bitcoin, la innovación de su tecnología y el impacto que su puesta en funcionamiento ha tenido sobre la manera de operar de los sistemas financieros a escala mundial. Para ello se revisan conceptos como blockchain, nonce, minería, encriptado o halving y se evidencia cómo el uso del dinero físico va retrocediendo a escala mundial. No obstante, el trabajo no solo se centra en el bitcoin y, también, revisa la evolución de distintas criptomonedas que se crearon y se siguen creando en la actualidad. Finalmente, el trabajo evalúa tanto las ventajas como desventajas que las criptomonedas presentan.

Palabras clave: Criptomoneda, blockchain, encriptado, bitcoin, token

Códigos de clasificación JEL: E42 y F02

ABSTRACT

This paper is aimed to analyze different aspects linked to the cryptocurrency phenomenon. The paper tries to answer some aspects such as what they are, how they were created, how they work, what they intend, how many there are, who creates them or what advantages they offer. To address all these questions, the paper begins by reviewing how the means of payment and the technology process have been evolving and the development of the philosophy that underpinned the creation of the first cryptocurrency, bitcoin. The paper continues to analyze how bitcoin works, the innovation of its technology and the impact that its implementation has had on the financial systems of different countries. To do it, concepts such as blockchain, nonce, mining, encryption or halving are reviewed. Likewise, it is evident how the use of physical money is going backwards on a global scale. However, the work is not only focused on bitcoin and also reviews the evolution of different cryptocurrencies that were created and continue to be created today. Finally, the paper evaluates both the advantages and disadvantages that cryptocurrencies present.

Keywords: Cryptocurrency, blockchain, encryption, bitcoin, token

1. METODOLOGIA

Para la realización del trabajo se han seguido distintos manuales que integran elementos sobre la aparición, evolución e impacto de las criptomonedas. También han sido visitadas distintas páginas web con objeto de analizar y obtener datos actuales sobre las criptomonedas examinadas.

2. INTRODUCCION

Es innegable el desarrollo exponencial de la tecnología en la última década del siglo pasado que continua en la actualidad. Este desarrollo ha potenciado un cambio, sin precedentes, en la vida económica, financiera, social del ser humano. Ahora somos capaces de interrelacionar sin contacto físico, pero sí visual y auditivo, con varias personas simultáneamente localizadas en distintos puntos geográficos muy alejados entre sí. Podemos enviarnos ciertos productos como fotografías, música, películas o estudios, ya sean científicos o no, en segundos. Asimismo, podemos enviar dinero desde un punto cualquiera del planeta a otro por muy lejano que esté. En esta dinámica aparece una nueva forma de abonar cantidades monetarias por un producto o servicio. Son las criptomonedas, también denominadas por el sinónimo criptodivisas o monedas virtuales, que carecen de soporte físico y sus movimientos sólo se realizan utilizando la red.

Detrás de las criptomonedas hay un potente desarrollo tecnológico, pero no solo eso, pues también su estructura y dinámica sigue un protocolo estricto diseñado por distintos creadores. El protocolo de funcionamiento tiene por objetivo potenciar la confianza de los consumidores de modo que tiendan a utilizarlas para el pago de bienes y servicios. La base de la subsistencia de las criptomonedas es la confianza, aunque este aspecto no es característico sólo de las criptomonedas ya que también, este aspecto, es la base de la circulación del dinero físico.

El objetivo de este trabajo es sintetizar cómo funcionan las criptomonedas, su impacto en los consumidores y analizar las ventajas y desventajas de su utilización. En suma, se pretende abordar distintos aspectos ligados a las criptomonedas utilizando información obtenida desde Internet y distintas publicaciones. La contribución del trabajo, frente a otras, sería agrupar en un mismo contenido los aspectos más importantes de las criptomonedas. Con ello se pretende una mejor comprensión de su funcionamiento, de su utilidad y de su impacto.

El trabajo está dividido en secciones. Después de esta introducción, la segunda sección se ocupa de distintas definiciones de criptomonedas. En la siguiente se hace un breve resumen de cómo ha ido evolucionando el pago de bienes y servicios. En la cuarta se repasa la tecnología bitcoin, donde se explica el trabajo de los mineros, qué es el nonce o la tecnología blockchain. La quinta sección repasa la tecnología bitcoin. La siguiente se ocupa de la historia del bitcoin, como nace y porqué. Posteriormente, se estudia la dinámica del precio

del Bitcoin en relación al euro. La evolución del precio del bitcoin es la introducción a otras criptomonedas, donde se muestra la evolución de sus precios frente al euro. De alguna forma, la sección siguiente resume las las características más destacables de las criptomonedas, terminando el trabajo con unas conclusiones finales.

3. MONEDAS VIRTUALES

En octubre de 2012 (pp.13), el Banco Central Europeo (BCE) proporcionaba una definición sobre las monedas virtuales. Se establecía que "una moneda virtual es un tipo de no regulada, moneda digital, que es emitida y usualmente controlada por sus desarrolladores, y utilizada y aceptada por los miembros de una específica comunidad virtual". El BCE aceptaba que era posible modificar la definición anterior alertando de que futuros acontecimientos podrían alterarla. En 2014 (pp.11), la Autoridad Bancaria Europea (ABE) indica que "una moneda virtual puede definirse como una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda de curso legal, que no tiene la consideración de moneda o divisa, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos".

Siguiendo a Schueffel et al. (2019), las criptomonedas o criptodivisas son monedas virtuales, consecuentemente se utilizan para intercambiar bienes y servicios. Los mismos autores señalan que, a diferencia del dinero fiduciario, su tráfico está descentralizado y no requiere la presencia de un intermediario. Las criptomonedas son independientes de organismos gubernamentales o financieros. Consecuentemente, las intervenciones que estos organismos pudieran acometer, no tienen influencia sobre las criptomonedas.

La independencia de una moneda virtual puede resultar muy atractiva para realizar pagos, pero también puede ser utilizada para evadir impuestos, blanquear dinero y comerciar con bienes ilícitos. Este último aspecto señalado por Brito, J. y A. Castillo (2013) es el que ha llevado a la red FinCeN (FinancialCrimesEnforcement Network) en los Estados Unidos a solicitar una regulación de las monedas virtuales. En marzo de 2013 esta red delimitaba el concepto de moneda real y virtual estableciendo que "una moneda virtual es un medio de intercambio que opera como una moneda real en ciertos entornos, pero no tiene todos sus atributos" especialmente señala como diferencia la base legal.

Como apunta Schueffel et al., una criptomoneda utiliza la criptografía para controlar la emisión de nuevas unidades y verificar la transferencia de fondos. La criptografía podría definirse como la materia que estudia algoritmos, protocolos y sistemas con la intención de dar seguridad a las comunicaciones, a la información y a las entidades que se comunican. La criptografía es un aspecto importante al considerar las monedas virtuales ya que las

transacciones tienen que ser extremadamente seguras al carecer de cualquier supervisión.

En 2009, apareció el bitcoin siendo la primera criptomoneda completamente descentralizada. Se asegura que el bitcoin fue creado por Satoshi Nakamoto que corresponde a un seudónimo, desconociéndose en la actualidad quién la persona que utilizó este seudónimo[1]. No obstante, el anonimato es parcial ya que la filosofía subyacente en el bitcoin coincidía con muchas ideas desarrolladas en la comunidad cypherpunk. Esta comunidad estaba formada por personas especializadas en la criptografía informática como Jacob Appelbaum, Andy Müller-Maguhn o JérémieZimmermann, todos ellos contribuyeron en el libro de Julien Assange, el fundador de WikiLeaks.

También, parece importante destacar que Satoshi Nakamoto no creo toda la tecnología Bitcoin pues mucha de la tecnología utilizada se basaba en investigaciones previas que se habían ido desarrollando loa años anteriores. No obstante, Bitcoin mejoraba y ampliaba toda la tecnología que se había desarrollado hasta 2009 para el comercio electrónico.

4. PATRONES EN EL INTERCAMBIO DE BIENES Y SERVICIOS

Parece necesario realizar un breve repaso sobre cómo han ido evolucionando las transacciones de bienes y servicios para así entender como se ha llegado a la utilización de las criptomonedas.

El análisis puede comenzar en el Neolítico que es cuando los historiadores parece que están de acuerdo en aceptar el periodo como la época en aparecieron excedentes alimentarios como consecuencia de la aparición de la agricultura. Con los excedentes se podría comerciar y conseguir bienes que, normalmente, estaban dentro de la esfera de los deseos y fuera de la esfera de las posibilidades. Los deseos podrían ser el motivo de los intercambios de unos bienes por otros. Sin embargo, los intercambios generaban ciertos problemas que las monedas trataban de paliar. La aparición de la moneda era un procedimiento para determinar qué cantidad de un bien era equitativa si trataba de cambiarse por otro bien o por el servicio de trasladar los bienes de un lugar a otro. La Figura 1 contiene las relaciones causa efecto desde el intercambio del Neolítico a la utilización de las criptomonedas.

Las monedas tendrían que tener un valor intrínseco de modo que se aceptasen, sin reservas, en el intercambio entre un bien o servicio por ellas. Realmente parece que fue difícil encontrar una moneda admitida por todo el mundo como medio de pago ya que se utilizaron dientes de ballena y hasta esclavos para los abonos. Finalmente, lo que mejor se admitió fueron las monedas manufacturadas con metales preciosos, como el oro, la plata o la unión de ambos. Pero la gente tenía que trasportar y almacenar oro y

[1] Se desconoce si es una persona o un grupo, si es un hombre o una mujer.

empezaron a confiar el oro a los joyeros, que lo guardaban en sus cajas fuertes y emitían unos papeles que equivalían a cierta cantidad de oro. De este modo, la gente empezó a confiar en aquellos papeles que estaban respaldados por ciertas cantidades de oro. Es lo que se llama patrón oro (ver Figura 1) y se emitían monedas construidas con metales de no mucho valor pero subyacía en ellas un valor determinado de modo que cada unidad monetaria estaba determinada en términos de equivalencia con una cantidad específica de oro.

Sin embargo, la libre emisión de los papeles por parte de cada país originó que, tras la primera guerra mundial, Alemania, que necesitaba mucho dinero para poder reparar los daños causados por la guerra, emitiese mucho de ese dinero, lo que dio lugar a un proceso de hiperinflación[2] y la confianza en el respaldo de este dinero se resquebrajó. Para eliminar este inconveniente, se centralizó y se controló la creación de estos papeles que dejaron de estar respaldados por un intercambio de los mismos por oro. Ahora únicamente servían, y aun sirven, porque sabemos que otras personas aceptaran esos mismos papeles con el valor que tienen asignado cada uno de ellos, es decir, su base es la confianza.

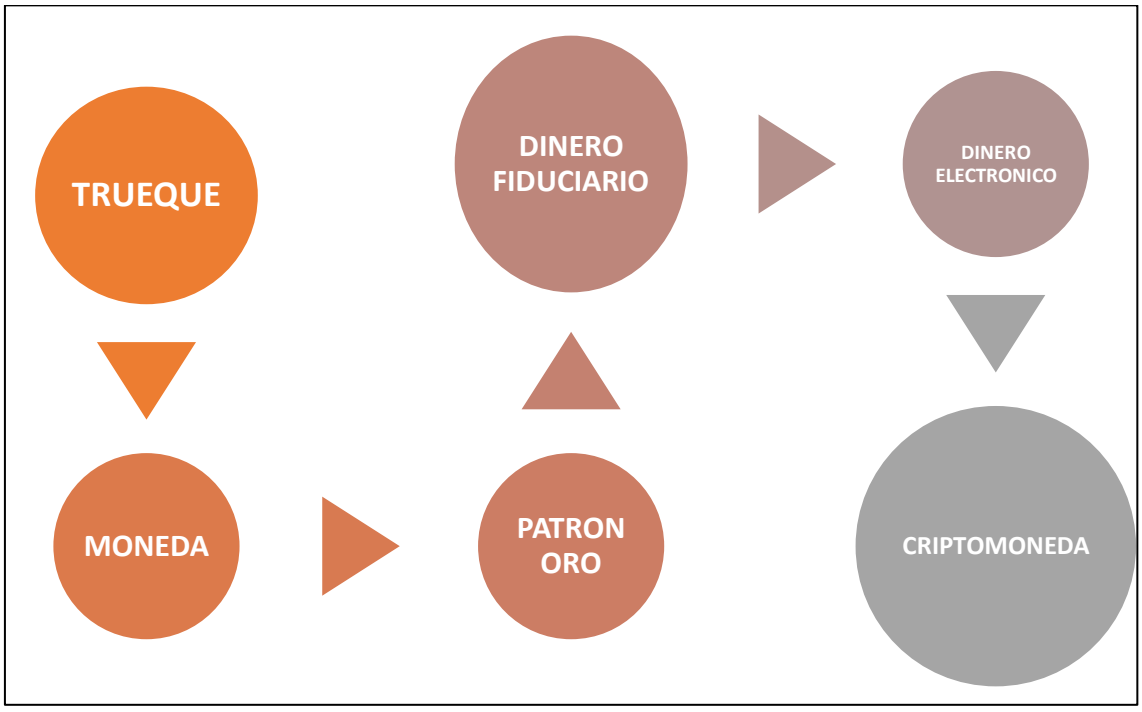


Figura 1: Relaciones causa-efecto en la aparición de las criptomonedas.

Con el paso de los años, el avance de la tecnología ha permitido que se puedan realizar compras sin necesidad de ir físicamente al lugar donde se venden o sin tener que llevar el dinero en efectivo para pagarlos. En 1958

[2]Uno de los objetivos del Banco Central Europeo es la estabilidad de precios. En 1998 se definió: "La estabilidad de precios se define como un incremento interanual del índice armonizado de precios de consumo (IAPC) de la zona del euro inferior al 2%. La estabilidad de precios ha de mantenerse en el medio plazo".

(www.bbva.com), se creó la tarjeta[3] VISA y aunque han ido evolucionando, es la base de la que utiliza en la actualidad.

Cuando surgieron las tarjetas todas funcionabas con la tecnología de la banda magnética. En la actualidad, esa tecnología ha sido superada, y casi todas funcionan con un chip o son contacless. La tecnología contacless ha mejorado la seguridad ya que no hace falta que la tarjeta se aleje de la mano de su poseedor con lo que la copia de la tarjeta es mucho más difícil. La difusión de las tarjetas es un éxito ya que en la actualidad, siguiendo a Europa Press (www.eleconomista.es, enero, 2018) el 82% de la población española tiene tarjeta, incluso más de una. Realmente, la utilización de las tarjetas ha estado potenciada por las entidades financieras ya que muchas de ellas tienen asociada una tarjeta a una cuenta de modo que la tarjeta es un requisito para tener activa la cuenta. Adicionalmente, para evitar ciertas comisiones bancarias, las entidades financieras obligan a utilizar sus tarjetas un número determinado de veces al mes. La figura 2 muestra la evolución del pago con tarjetas en España. El soporte de la tarjeta también ha evolucionado, ahora los dispositivos móviles como Smartphone o los Smartwhatch permiten llevar toda la información de las tarjetas e incluso pagar con ello simplemente acercando el dispositivo a la pantalla o al cajero para obtener efectivo en moneda fiduciaria.

La prensa (www.bbc.com) proporciona información de que el efectivo es cada vez menos utilizado en muchos países europeos. Holanda intenta que la utilización del dinero en efectivo sea menor del 40% en los pagos en supermercados, Dinamarca, Suecia o Italia abogan por medidas similares. Muchas asociaciones pretenden eliminar el efectivo y que la gente pague, aunque sean cantidades muy pequeñas, con dinero electrónico. En Suecia uno de los medios de pago más utilizados y que más empuja a la eliminación del dinero en efectivo es el llamado sistema swish, tanto lo utilizan allí que han llegado a crear de manera coloquial el verbo swishear como sustitutivo del verbo pagar. Este sistema cuenta con 7,5 millones de usuarios, que teniendo en cuenta la población de Suecia (10,12 millones de personas), implica que el 74% de la población utiliza o ha utilizado este método de pago.

Esta aplicación también existe en España con el nombre de Bizum que consiste en el traspaso de dinero entre cuentas solo con la posesión del número de teléfono de la persona que va a recibir el dinero, teniendo cada persona su número de teléfono asociado a su cuenta bancaria personal. Ahora mismo, Bizum, permite el traspaso de hasta 2.000 euros, e incluso da la posibilidad de pedir dinero a alguien a través de este sistema.

En la página www.bizum.es se encuentra que el número de usuarios con los que cuenta esta compañía de servicios de pago y las transacciones es alrededor de 6,6 millones de usuarios en 2009 y 83 millones de transacciones, es decir que en menos de 4 años desde su aparición, aproximadamente el 14,15% de la población lo utiliza o lo ha utilizado. El sistema Bizum está

[3] En España, las tarjetas comenzaron al principio de los sesenta.

presente en el 96% de las entidades bancarias que operan en España e incluso están sumándose empresas a las que se puede pagar facturas con este tipo de transacción, por ejemplo la compañía Iberdrola.

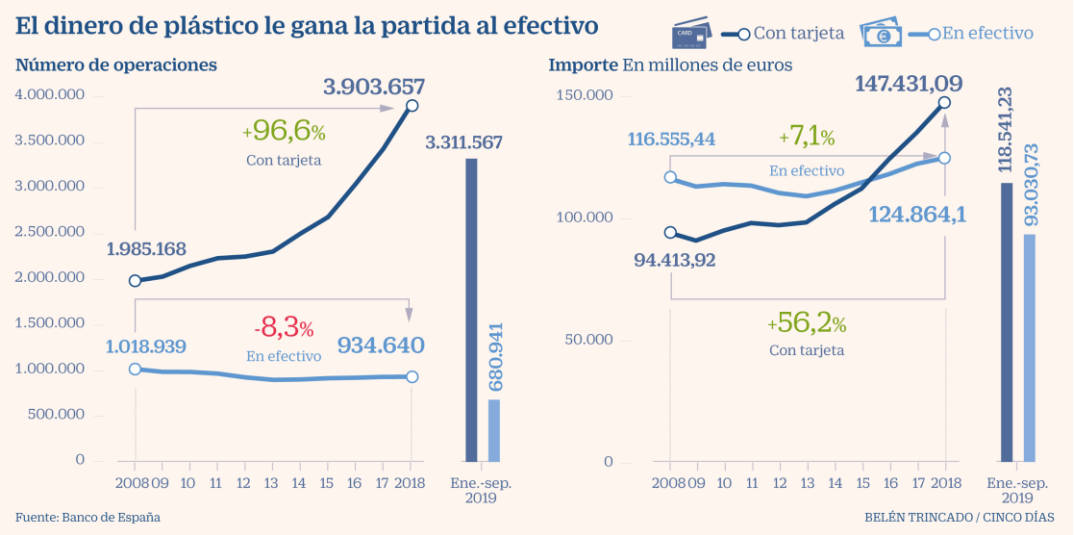


Figura 2: Evolución de los pagos con tarjeta en España

Fuente: Cinco Días (diciembre, 2019)

Para terminar las relaciones causales que son recogidas en la figura 1 se establece la relación causal entre dinero electrónico y criptomonedas. Para analizar esta influencia se tiene en cuenta el marco de la crisis financiera de 2008. La crisis, que comenzó en EEUU en 2006 pero terminó por infectar al resto de las economías del mundo, fue debida a la burbuja inmobiliaria relacionada a las hipotecas subprime que impulsó una crisis de liquidez y un derrumbe bursátil en 2008. Esta crisis reforzó la idea de la fragilidad del sistema monetario establecido y pudo influir en la creación de la primera criptomoneda en 2009. Entonces, parece que su creación trataría de formar un medio de pago sin un banco central que lo controle y organismos que tomen decisiones que afectan a todos los que poseen las monedas. Ese objetivo pudo condicionar las ideas de su creador que puso en circulación una moneda que no pertenece a ningún organismo, sino a todos los que la utilizan.

5. TECNOLOGÍA BITCOIN

La tecnología Bitcoin no se formó desde la nada. En la década de 1970, se comenzó a utilizar las firmas digitales, que permitían al receptor de un mensaje conocer quién mandaba un mensaje y tener la seguridad de que el mensaje no había sido alterado en el camino desde el envío hasta la llegada. Las firmas digitales están basadas en la criptografía de clave pública o criptografía de dos claves que obliga a utilizar dos claves para el envío de un mensaje, una es

pública y otra sólo es conocida por el usuario. Estas tecnologías eran progresivamente mejoradas y se descubrían otras nuevas. Por ejemplo, antes del Bitcoin se utilizaban tecnologías de efectivo electrónico desarrolladas por David Chaum, quién es considerado como el inventor del dinero digital seguro, y Stefan Brands que abogaba por métodos para disminuir costes en las transacciones electrónicas de pagos.

En este breve repaso de la evolución de la tecnología debe de incorporarse a Adam Back quien en 1997 desarrolló el hashcash para combatir el correo basura también conocido como spam. El hashcash es un mecanismo de prueba de trabajo que incorporó la tecnología Bitcoin. La figura 3 muestra la utilización de los hash en la tecnología Bitcoin que puede encontrarse su funcionamiento pormenorizado en satoshin@gmx.com.

El objetivo de la tecnología Bitcoin es identificar y validar las transacciones de esta moneda. Siguiendo a M. Gates (2017), la tecnología Bitcoin podría sintetizarse en un solo aspecto: cómo se manejan las transacciones de la criptomoneda. Una transacción tiene entradas y salidas para determinar de dónde proviene la criptomoneda y hacia dónde va. Las transferencias se agrupan en bloques. Cada bloque tiene tres elementos: una marca de tiempo, un número de verificación y una identificación del bloque anterior. Los bloques los generan especialistas en la tecnología, que son conocidos como mineros, y antes de crearlos verifican la validez de todas las transferencias. Una transferencia que se ha quedado fuera de la cadena de bloques no es válida y una transferencia dentro de la cadena se considera válida.

Cuando un nodo, esto es, un ordenador, conectado a la red Bitcoin genera un bloque, se lo comunica al resto de nodos quienes verifican que es válida su construcción. Si se da por aceptado el bloque, se empezará a trabajar en él convirtiéndose en el final de la cadena de bloques. Parece evidente la posibilidad de que dos bloques se creen a la vez. Entonces, se conservan los dos bloques pero aquel que más crezca será el que se mantenga y el otro terminará por desecharse.

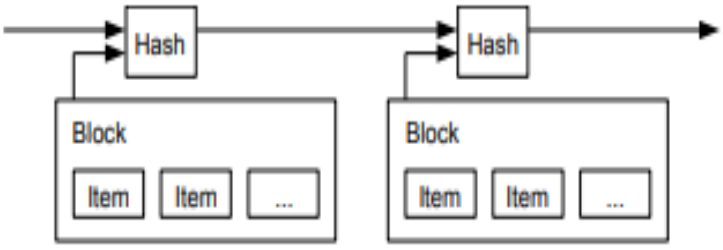


Figura 3: Hash en la tecnología bitcoin

Fuente: satoshin@gmx.com

La creación de bloques en la tecnología Bitcoin está diseñada para evitar que puedan realizarse transacciones no correctas o no honestas. Se vigila sólo un cierto número de bloques y para limitarlos utiliza lo que se conoce como prueba de trabajo (*proof-of-work)* también denominada PoW*.* La prueba de trabajo consiste en que la creación de un bloque lleva tiempo y, por tanto, un nodo tiene que tener mucho tiempo para poder crear muchos bloques. Este sencillo procedimiento limita el número de bloques que puede crear un nodo. Además, para crear un bloque hay que encontrar lo que se conoce como el nonce, un número de verificación, de tal forma que el hash del bloque sea menor que un determinado valor, al que se denomina valor objetivo. El nonce se busca por la técnica de prueba y error. Se empieza por cero y se calcula el hash. Si es menor que el objetivo, ya se tiene el nonce; en caso contrario se aumenta la selección original en cierta cantidad y se vuelve a iterar el proceso hasta que se encuentre el nonce. La probabilidad de encontrar el nonce es muy pequeña ya que el valor objetivo se selecciona de tal forma que generar un bloque supone unos diez minutos. Para que los diez minutos se mantengan en el tiempo, aproximadamente cada dos semanas se recalcula el valor objetivo.

El primer nodo o lo que es lo mismo, el primer minero, en encontrar el nonce obtiene, en la actualidad, 12,5 monedas siempre y cuando los demás usuarios confirmen que la respuesta del minero es acertada. Realmente, son los mineros los que sustentan la red bitcoin que trabajan por las 12,5 monedas con una probabilidad pequeña de conseguirlas. Lo que se conoce por blockchain es precisamente la red de bloques. La alta seguridad que ofrece la tecnología blockchain, o cadena de bloques, trata de adaptarse, en la actualidad, a otros ámbitos siempre que impliquen cualquier tipo de transacción. En realidad, la alta seguridad que conlleva la cadena de bloques es por lo que se considera esta tecnología de utilidad en numerosos ámbitos ya que infectar una red de bloques parece excesivamente complicado ya que se tendría que infectar bloque a bloque.

Un problema en la tecnología bitcoin es el espacio de almacenamiento que se requiere para guardar los bloques. Por este motivo, muchos bloques se desechan para intentar reducir el espacio. De un modo sencillo puede decirse que la tecnología intenta reducir ese espacio y por ello desecha bloques que no van a volver a ser útiles y solamente guarda los que se vayan a utilizar.

Además del potente sistema tecnológico en el que se basa la criptomoneda, hay un protocolo de actuación. Por ejemplo, la tasa a la que se liberan nuevos bitcoins está controlada de tal forma que, aproximadamente, cada 4 años se reduce en el 50%. Con esta forma de actuar se logra el efecto escasez característico de cualquier moneda. Está calculado que el número de bitcoins en circulación nunca pasará de los 21 millones lo que ocurrirá en el año 2140.

Los mineros no siempre obtendrán 12,5 bitcoins y cada 35.000 horas, que son aproximadamente 4 años, o lo que es lo mismo después de crear 210.000 bloques, hay un halving que reduce a la mitad la paga de los mineros por hacer el bloque. Los halvings se ejecutarán de forma automática, de acuerdo a lo establecido en el código Bitcoin. No obstante, a partir de ese momento, por cada bloque minado se emitirá la mitad de Bitcoins al mundo y los mineros

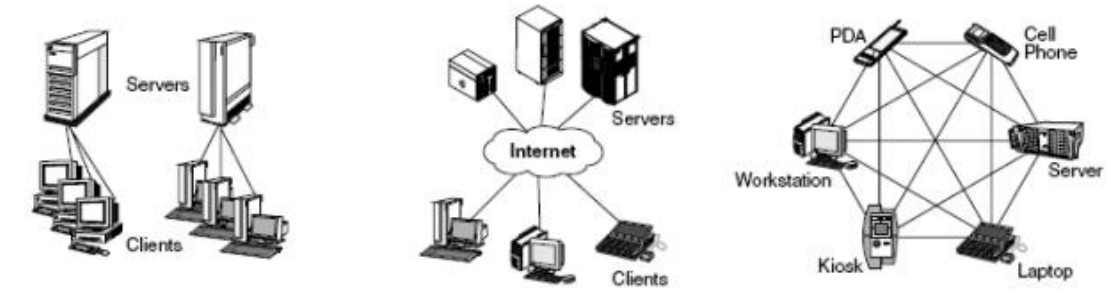
recibirán la mitad de bitcoins por su trabajo. De hecho en 2140, después de minar el bloque 6.930.000, los mineros trabajarán por las comisiones ya que el sistema no les proporcionará bitcoins. En www. academy.bit2me.com se estima la fecha de los diferentes halvings, que serán 34 en total.

El tercer halving del bitcoin se completó el 11 de mayo aproximadamente a las 21:21 hora española, de acuerdo a la información proporcionada por el periódico digital Bolsamanía en su publicación del 1 de julio de 2020. Los mineros pasarán a cobrar 6,25 bitcoins por bloque completado. El análisis técnico pronosticaba que con cada halving, el precio del bitcoin subiría pero en este caso no ha habido tal boom y cotiza en junio en una banda de 8.300 a 8.700 dólares.

6. ALGUNOS DATOS SOBRE LA HISTORIA DEL BITCOIN

El comienzo del bitcoin fue el 1 de noviembre de 2008 cuando un mensaje fue enviado a la lista de correo sobre criptografía de metzdowd.com firmado con el alias de Sathosi Nakamoto y titulado Bitcoin P2P e-cash paper. En el mensaje se describía un nuevo sistema de efectivo electrónico llamado Bitcoin. El sistema tenía una red peer-to-peer, lo que significa que es una red de ordenadores en la que todos los participantes se relacionan como iguales. La figura 4 muestra la diferencia de trabajo entre internet y bitcoin con el sistema P2P.

El sistema peer to peer que incorpora la tecnología bitcoin permanece disponible en la dirección web /www.bitcoin.org/bitcoin.pdfy en el que se explica el funcionamiento del protocolo propuesto.



a. Client-server stacks with limited interoperability and homogeneous client and server systems

b. Web-based computing supports heterogeneous clients and servers

c. Peer-to-peer computing enables direct communication between peers and new interaction styles

Figura 4: Diferentes tecnologías de comunicación

Fuente: M. Disanzo (Redes Peer to Peer y Tecnología JXTA)

El 3 de enero de 2009 se pone en funcionamiento la primera red peer-to- peer después de poner en marcha el software de código abierto, esto es, software sobre el que pueden actuar usuarios por la disponibilidad de su código fuente.

Un código fuente es el que dice al ordenador lo que tiene que hacer para que el software funcione. El 3 de enero de 2009 se empezó a hacer el primer bloque que supuso la creación de las primeras monedas bitcoins y el inicio de la minería. El primer bloque de bitcoin, llamado el bloque de génesis, fue minado por el propio Satoshi Nakamoto.

El programador HalFinney (1956-2014) fue la primera persona en adoptar, apoyar y contribuir al bitcoin, además, descargó el software bitcoin el día en que fue lanzado y recibió 10 bitcoins de Nakamoto, lo cual fue también la primera transacción bitcoin del mundo. Otros de los primeros adoptantes fueron WeiDai, creador de b-money, un sistema de intercambio de valor que nunca llegó a funcionar y Nick Szabo, creador de Bit Gold una moneda digital que tampoco llego a existir, ambos predecesores de bitcoin

Las primeras transacciones de la moneda tuvieron lugar entre individuos en el foro Bitcointalk, con una notable transacción de 10 mil bitcoins usados para comprar indirectamente dos pizzas entregadas por Papa John's. En los primeros días, se estima que Nakamoto minó un millón de bitcoins.

Antes de desaparecer, Nakamoto entregó la gestión del proyecto y el repositorio original a Gavin Andresen, quien luego se convirtió en el desarrollador líder de la Fundación Bitcoin[4] creada en 2012. La Fundación Bitcoin es una organización sin ánimo de lucro que pretende la estandarización, protección y promoción del protocolo del software abierto, adicionalmente pretende que el bitcoin represente a una economía que no dependa de la política, sea abierta e independiente. Además de Gavin Andressen, sobre el que no se sabe ni en qué fecha nació, fundaron la fundación el economista Jon Matonis, Patrick Murck que posee las patentes para quitar el anonimato de las transacciones Bitcoin, Charlie Shrem que estuvo involucrado en una operación de lavado de dinero con criptomonedas y Peter Vessenes que posee la patente fundamental para quitar el anonimato de las transacciones Bitcoin.

También en esta historia se pueden señalar algunos fallos importantes de la tecnología. El 6 de agosto de 2010, se detectó que las transacciones no se verificaban adecuadamente antes de ser incluidas en la cadena de bloques, lo que permitía eludir las restricciones de Bitcoin y crear un número indefinido de bitcoins. Nueve días más tarde se generaron más de 184 mil millones de bitcoins en una transacción y se enviaron a dos direcciones en la red. En cuestión de horas, la transacción se detectó. Este problema se solucionó cuando se puso en marcha una nueva versión del bitcoin. Este suceso se considera como el único fallo serio de seguridad de la tecnología Bitcoin. Obviamente, la tecnología no es totalmente segura y fallos de distinta envergadura pueden haber ocurrido e incluso pueden haber sido detectados aunque no publicados.

[4] En www.criptonoticias.com se puede encontrar el artículo de M. Vanci, “Auge y caída de la Fundación Bitcoin: la organización detrás de los escándalos”, de septiembre de 2019, donde se repasa los avatares de esta organización.

7. DINÁMICA DEL PRECIO DEL BITCOIN

Un bitcoin como las monedas fiat es divisible y está compuesto de 100 millones de céntimos. Cada céntimo se llama satoshi en honor del creador de la tecnología. De este modo es posible comprar satoshis donde vendan bitcoins con un desembolso más asequible dado el actual precio del bitcoin.

En España, los bitcoins[5] se pueden comprar en plataformas como coinbase, kraken o BitFitness para grandes volúmenes. En CoinMarketCap.com se puede encontrar los precios, el volumen de transacciones, la oferta circulante y el cambio que se están pagando por los bitcoins en cada momento. También se puede adquirir bitcoins en cajeros automáticos disponibles en ciertas ciudades. Evidentemente, se pueden comprar a personas que quieran venderlos, LocalBitcoins.com es una plataforma donde se puede interactuar con compradores y vendedores de pequeñas cantidades.

Desde luego, los bitcoins pueden ser utilizados para adquirir bienes y servicios siempre que la contraparte los acepte. No obstante, hay muchos especuladores de bitcoins de la misma forma que hay especuladores en metales preciosos o en divisas. Distintas páginas de Internet aconsejan que en caso de que se vaya a especular en bitcoins su almacenamiento sea en frio, lo que significa que hay que guardar las claves privadas fuera de Internet para no ser atacadas por los hakers.

En el mundo, no hay una plataforma única para transacciones de bitcoins y el precio no es único pudiendo haber pequeñas diferencias que como en el caso de las monedas fiat las diferencias suelen ser aprovechadas por intermediarios para obtener altas rentabilidades.

El precio de los bitcoins se rige por la ley de la oferta y la demanda. Los mineros, como parte del mercado, también influyen en el precio. Si el bitcoin tiene un precio bajo, muchos mineros abandonan la creación de bloques pues la recompensa del trabajo es pequeña y se ralentiza la emisión de nuevos bitcoins. Un bitcoin (BTC) comenzó valiendo 0$ y en julio de 2010 su valor era de 0,08$, en cinco días había subido un 1000% (datos tomados desde academy.bit2me.com). Su valor fue de 1$ en abril de 2011.

En el precio del bitcoin frente al euro se pueden distinguir cuatro etapas. La primera comprendería el intervalo que transcurre desde la aparición del bitcoin hasta 2014 donde el precio alcanza el valor medio de 827,6 euros en

[5] Para comprar monedas virtuales, hay que crear una wallet, esto es, un monedero digital donde se almacenan las monedas virtuales. La wallet permitirá, también, enviar divisas, recibirlas y acceder a las empresas Exchange. La wallet proporciona acceso a las blockchains de cada moneda virtual y pueden descargarse en el móvil. También se tiene la posibilidad de imprimir el código en formato papel o almacenarlo en memorias USB. El proceso de verificación de identidad de las empresas Exchange incluyen datos personales para mejorar su seguridad, requieren un proceso llamado KYC, cuyas siglas significan *know your customer.* La idea es mantener una política de conocimiento del cliente para la prevención del blanqueo de capitales.

noviembre de 2013. En esta etapa el crecimiento del precio no ha sido paulatino ya que ha tenido variaciones diarias aunque siempre inferiores a 100 euros. Esta etapa es un periodo extenso con un crecimiento de precio muy lento que corresponde a una etapa de nacimiento. Muchos analistas justifican (btcdirect.eu/es-es/precio-bitcoin) la evolución en esta etapa al desconocimiento, por parte de especuladores, del potencial de las criptomonedas. No obstante, también, podría ser consecuencia de la escasez de confianza en ellas que fue progresivamente aumentando con el tiempo como puede comprobarse con la actitud mostrada después del problema de Chipre. La problemática fue que Chipre sufrió una crisis financiera a causa de un aumento desmesurado de su desempleo así como por una bajada importante en su PIB. La situación fue tal magnitud que Chipre necesitó ser rescatada tanto por el FMI como por la UE (www.bbc.com/mundo/noticias/2013/03/130322_chipre_rescate). El resultado de la crisis fue la creciente desconfianza de muchos inversores y especuladores en el sistema establecido y por ello buscaron las alternativas que ofrecían las criptomonedas.

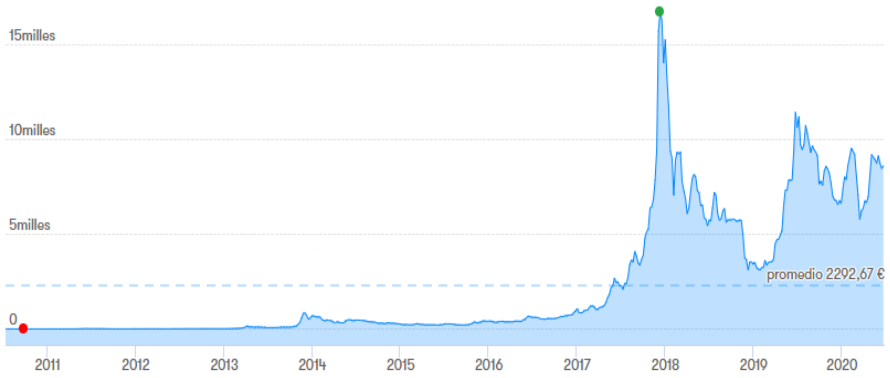


Figura 5: Evolución del cambio bitcoins/euros

Fuente: https://btcdirect.eu/es-es/precio-bitcoin

Una segunda etapa transcurriría desde 2014 hasta 2017 que podríamos denominar la etapa de la consolidación del precio. Arranca con un precio medio de 827,6 euros alcanzando los 948, 74 euros en diciembre de 2016. Estos dos valores se convierten en barreras durante esta etapa ya que nunca el precio sale de la franja, aunque diariamente hay fluctuaciones en los precios. En esta etapa es cuando el mercado sufrió la bancarrota de Mt. Gox que era una de las plataformas de intercambio de bitcoins de las más grandes del mundo. La plataforma se creó en 2010 con sede en Shibuya (Tokio). La importancia de la plataforma es evidente al constatar que logró manejar hasta un 70% de todas

las transacciones realizadas en bitcoins. A principios de 2014, Mt. Gox[6] manifestó que más de 850.000 bitcoins habían sido hackeados de sus cuentas, lo que representaba en ese momento unos 470 millones de dólares y la compañía fue forzada a iniciar su proceso de liquidación. La desaparición de Mt. Gox[7] tuvo un serio impacto sobre el bitcoin que paso de tener un valor cercano a 1.000 euros a costar unos 300 euros al final del año. Un año después, en enero del 2015, el precio cayó a unos 180 euros como consecuencia de otro importante hackeo de 19.000 bitcoins que sufrió el tipo de cambio líder en Europa, el Bitstamp (www.bitstamp.net), con sede en Luxemburgo.

Una tercera etapa iría desde enero de 2017 con una cotización media de 1.074, 34 euros hasta enero de 2019 con una cotización media de 3.113, 09 euros. A diferencia de lo que ocurrió en la segunda etapa, en esta etapa, las cotizaciones son dos mínimos. Desde enero de 2017, el precio comienza a escalar alcanzando un precio que es el más alto de la historia del bitcoin 16.727,68 euros en diciembre de 2017. Hay que tener en cuenta que el bitcoin subió desde septiembre de 2017 hasta diciembre de ese año 13.372,93 euros. Alcanzado el pico, el precio comenzó a descender hasta cotizarse al precio dado en enero de 2019. Es cierto que el descenso fue rápido pero había cambios de tendencia desde mínimos en febrero, junio, agosto y septiembre de 2018. Este comportamiento del precio rara vez se produce en los mercados y se justifica por el impulso de las recomendaciones de compra que se hacían desde distintos medios financieros.

El 2018 se considera un año de corrección para esta criptomoneda. En ese año, el bitcoin llegó a tener un precio de poco más de 3.100 euros como consecuencia de caídas en cascada que se genera mediante cadenas de procesos causa-efecto. Así cada leve descenso del precio del bitcoin desencadena ventas por doquier debido a la ruptura de inversiones, lo que genera mayores caídas.

En enero de 2019, el bitcoin permaneció en una zona de precios estabilizados durante unos cuatro meses para comenzar una nueva etapa alcista alcanzando un máximo en junio de 2019, con un precio medio de 11.406,17 euros que en la actualidad no ha sido superado. Desde el pico, el precio del bitcoin comenzó a caer aunque no de forma vertical como en 2017 y alcanzó nuevos máximos en agosto de 2019 de 10.304,68 euros, octubre de 2019 con 8.573, 12 euros y en febrero de 2020 con una cotización media de 9.528, 79 euros. En marzo de 2020 aparece una pandemia mundial que será analizada en un apartado de esta sección.

[6] El robo se dividió en dos partes. La primera se produjo en 2011 detectada cuando un usuario aún no identificado se hizo con 25.000 bitcoins. Se especula que el robo pudo ser interno. La segunda parte se produjo en 2014. En este caso, se robaron 744.408 bitcoins. Una auditoria interna de la Exchange concluyó que el robo se produjo durante años de manera discreta. Los activos jamás se devolvieron. Tras esto, en 2015, la empresa cerró.

[7] Una mayor información puede encontrarse en www.academy.bit2m2.com

Llegado a este punto parece importante destacar lo que la evidencia confirma y es que la volatilidad es una característica del precio del bitcoin, que en términos financieros significa riesgo, por tanto, la inversión aleja a algunos inversionistas y especuladores. La alta volatilidad podría justificarse por el tamaño del mercado de bitcoins que al ser pequeño, pequeños movimientos generan variaciones en todo el mercado. Siguiendo la serie histórica de precios se comprueba que sus movimientos están muy influidos por los medios financieros al proporcionar recomendaciones de inversión o desinversión. También noticias relacionadas sobre la posible regulación de la moneda por distintos gobiernos poniendo en duda su más destacada cualidad, también genera huidas masivas del sistema bitcoin. No obstante, la limitación de bitcoins circulando, que permite definirlo como un bien escaso, con mucha o poca utilidad, debe proporcionar un impacto de mantener o superar el precio.

Sin embargo, parece importante destacar que sería de gran utilidad que el ecosistema Bitcoin continúe evolucionando ya que conlleva la mejora de la potencia de la computación de la red y un aumento de innovación sin precedentes. Estas mejoras no llaman tanto la atención de los medios pero es lo que realmente interesa para que el mundo de las criptomonedas adquiera estabilidad.

6.1 El Covid y el precio del bitcoin

En el mes de diciembre de 2019 apareció un nuevo coronavirus SARS-CoV-2 (SARS síndrome respiratorio agudo severo). Este nuevo coronavirus SARS-CoV-2 produce la enfermedad grave conocida como COVID-19. El coronavirus tiene su origen en la ciudad de Wuhan, capital de la provincia de Hubei, en la República Popular de China. El peligro principal de este virus es su velocidad de transmisión, esto se debe a que se trasmite de persona a persona a través de pequeñas partículas de saliva que se emiten al toser, estornudar o incluso hablar; aunque también se puede contraer a través del contacto con superficies contaminadas.

A finales del año 2019 se informó de una serie de casos de neumonía por una causa desconocida. Las medidas para combatirlo comenzaron posteriormente. Para combatir al coronavirus los países han adoptado distintas medidas. Muchos decretaron que el confinamiento era la mejor opción para frenar los contagios. La primera cuarentena directa por la pandemia se produjo en la República Popular de China, donde el gobierno ordeno el encierro de la provincia de Hubei el 23 de enero del 2020. En aquellos países en los que se optó por la cuarentena se tomaron medidas que afectaron drásticamente a la economía anteponiendo la salud de los ciudadanos y la no propagación del virus que estaba produciendo miles de muertes.

Algunos países optaron por no realizar este confinamiento de manera forzosa, es decir aconsejaron a la población sobre cómo prevenir el virus y solicitaron a

los grupos de riesgo que limitasen sus salidas pero no impusieron norma alguna con el convencimiento de que cada persona crearía anticuerpos necesarios para combatir el virus y el miedo por el repunte económico que supone la paralización de un país.

La figura 6 muestra la evolución del precio del bitcoin en los últimos 6 meses. A comienzos de marzo, a costa de la pandemia, el bitcoin cayó de 8.050 euros a 4598,18 euros entre los días 6 y 13 de marzo, lo que indica una disminución de al menos un 43,2% del valor. Una vez pasado el boom inicial del pánico, el bitcoin comenzó su paulatina recuperación.

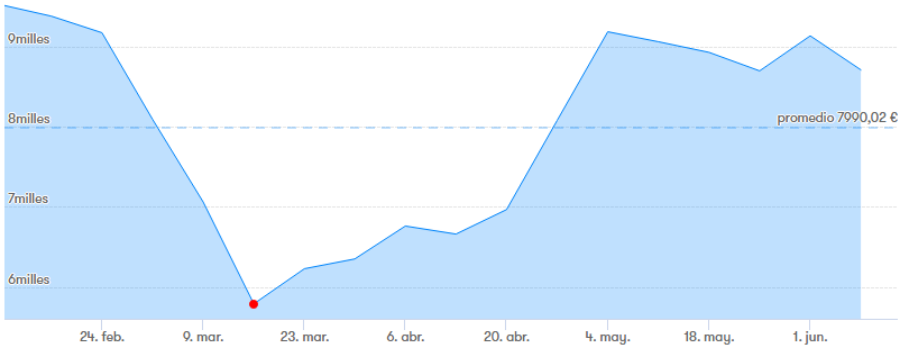


Figura 6: Cambio del bitcoins/euros en 2020

Fuente: https://btcdirect.eu/es-es/precio-bitcoin

Lo que nos asegura la figura 6 es que los poseedores de bitcoins se deshicieron de ellos con el inicio de la pandemia pero esto no ocurrió solamente con las criptomonedas, el oro, activo refugio por excelencia, el 16 de marzo alcanzó el precio de 1.300,87 euros un mínimo, aunque no tan brusco como el del bitcoin, ya que junio el precio medio del oro era de aproximadamente de 1.550 euros (www.inversoro.es). Las caídas fueron generalizadas en otros activos refugio, por ejemplo, el platino tuvo una caída el 16 de marzo que pasó a cambiarse a 18.764 euros frente a una media en junio de 22.500 euros.

Estos resultados parece que permiten concluir que los ciudadanos cerraron posiciones en todo tipo de inversiones y buscaron liquidez de dinero fiat, esto es, de aquel emitido bajo el paraguas de los gobiernos. Aunque desde luego no todos decidieron lo mismo, pues los activos siguieron cotizando.

8. OTRAS CRIPTOMONEDAS

En la actualidad existen más de tres mil tipos de criptomonedas que se diferencian por la tecnología que utilizan, por la encriptación y por la filosofía con la que operan. Pero antes de entrar en un pequeño análisis sobre cada una de ellas, se consideran dos conceptos ligados a las criptomonedas: altcoin y tokens.

- Altcoin es una palabra que recoge aquellas criptomonedas alternativas al bitcoin que se construyen desde el código fuente del bitcoin. Los altcoins tienen su propia cadena de bloques y su propia red P2P. No pueden utilizarse para adquirir bienes o servicios, aunque cotizan en mercados financieros cuyo precio sigue la ley de la oferta-demanda. Las altcoins se utilizan para financiar proyectos tecnológicos mediante las ICO, acrónimo de initial coin offer, esto es, ofertas iniciales de moneda. Los desarrolladores de un proyecto ofertan monedas que se compran en otras monedas virtuales y de este modo, se financia el proyecto cuyo éxito es incierto. Ejemplos de altcoins son Litecoin, Primecoin, que intenta encontrar nuevos números primos, o Darkcoin.

- Tokens es un nuevo término que www.bbva.com define como una unidad de valor emitida por una entidad privada. Es como un bitcoin pero engloba más aspectos. En una red privada, un token puede servir para pagar un servicio, permitir el acceso a determinados servicios, etc. Los tokens no tienen su propia cadena de bloques y son fáciles de crear. Se construyen sobre cadenas de bloques de criptomonedas ya existentes.

La multitud de criptomonedas existentes es consecuencia de las distintas preferencias de los inversores y de las diversas necesidades de los usuarios. Existen criptomonedas diseñadas para utilizarse en el intercambio de bienes y servicios siendo su objetivo final llegar a sustituir el dinero físico, este sería el caso del Bitcoin, Litecoin o Dash Otro tipo de criptomonedas podrían denominarse de utilidad como por ejemplo Ethereum cuya particularidad es que permiten ejecutar algoritmos más complejos. La criptomoneda Cardano es una mejora de los dos tipos anteriores haciendo de esta la criptomoneda una de las más completa. Esta sección, por último, estudia aquellas criptomonedas destinadas a la ayuda en las trasacciones, como puede ser Stellar o Ripple que en realidad no son criptomonedas pero si apoyan y financian sus plataformas con sus propias criptomonedas.

8.1 Litecoin

La creación del Litecoin[8] (LTC) se remonta al año 2011. Esta criptomoneda utiliza un algoritmo de cifrado de modo que la generación de bloques es cuatro veces más rápida que la del bitcoin. Fue creada por Charles Lie, titulado del Instituto tecnológico de Massachusetts, Universidad privada de Cambridge, EE.UU (MIT) y antiguo trabajador de Google.

El Litecoin no pretende competir con el Bitcoin, más bien está diseñado para llevar a cabo transacciones más pequeñas y rápidas que el Bitcoin. La emisión máxima de Litecoins está fijada en 84 millones.

La figura 8 muestra la evolución del precio del Litecoin en su cambio por euros desde su creación, donde se observa su parecido con la figura 7 ya que ambas monedas están afectadas por factores similares. El precio de los litecoins es

[8] La página Qué es Litecoin (LTC)? (www.criptonoticias.com) contiene mayor información.

mucho más bajo que las de los bitcoins. Consecuentemente, las fluctuaciones no afectan tanto a los poseedores de esta criptomoneda. Su valor máximo ha sido de 306 euros frente al valor del Bitcoin que como ya hemos comentado fue de 17.000 euros. Observamos que el precio del Litecoin no se ha recuperado desde la pandemia tan bien como lo ha hecho el Bitcoin.

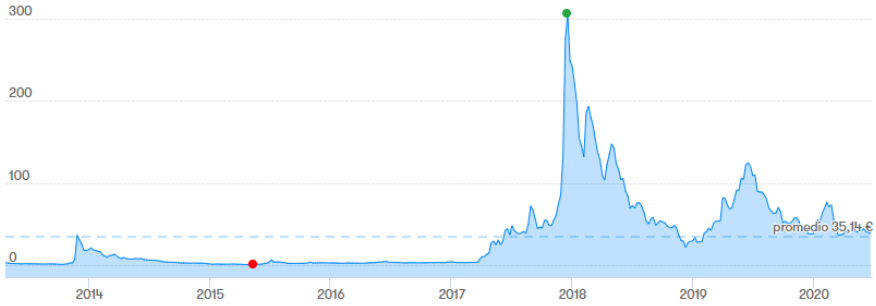


Figura 8: Evolución del cambio litecoins/euros desde su creación

Fuente: https://btcdirect.eu/es-es/precio-litecoin

8.2 Ripple

Esta moneda apareció por primera vez en 2012. Su objetivo es permitir transacciones financieras seguras, globales, instantáneas y casi gratuitas sea cual sea su tamaño. Hay diferencias entre Ripple[9] y XRP. Ripple es básicamente una compañía de pagos, mientras que XRP es la criptomoneda creada por Ripple para facilitar los pagos.

Ripple (XRP) no comparte con las criptomonedas algunos aspectos. En primer lugar, la moneda no está completamente descentralizada ya que está bajo el control de la empresa de Ripple Labs., lo que para muchos no es un punto a su favor pues el valor también depende de cómo funcione la empresa, sin embargo hay a quien le genera confianza tener una figura que le respalda. Otra de sus diferencias es que esta moneda no se puede minar, se crearon 100 mil millones de XPR a su inicio y ese es el límite de la criptomoneda. De la emisión de los 100 mil millones, 20 mil millones fueron retenidos por los creadores Chis Larsen (director de Ripple Labs.y afectado por el Covid-19) y Jed McCaleb, mientras que el resto fue entregado a Ripple Labs para su venta.

Si bien la plataforma dedicada a las transacciones ha tenido beneficios y valoraciones económicas muy positivas, la XRP no, esto se debe principalmente a que se generan ventas masivas de XRP para poder financiar la empresa Ripple Labs. En el largo plazo se espera que la mejora de la empresa Ripple Labs haga que el valor tanto de la misma como de XRP aumente. Por el momento según podemos concluir de la figura 9, el precio de

[9] Muchos datos sobre Ripple pueden encontrarse en Qué son y en qué se diferencian los Ripple? (www.academy.bit2me.com)

XRP respecto al euro es bajo comparado con otras criptomonedas. Su valor máximo ha sido de 2,5 euros.

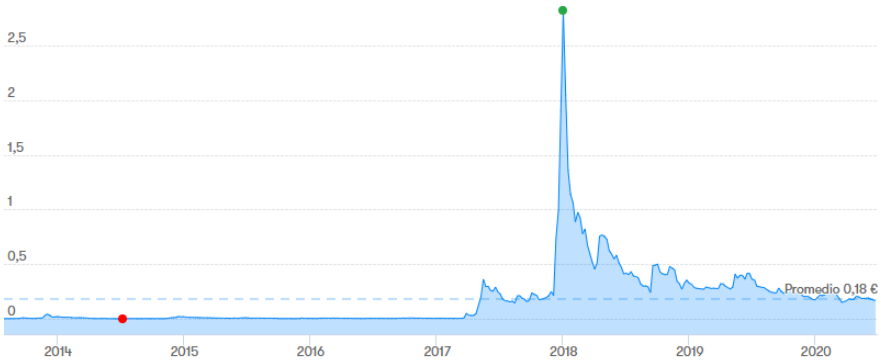


Figura 9: Evolución del cambio ripples/euros desde su creación.

Fuente: https://btcdirect.eu/es-es/precio-ripple

8.3 Dash

La criptomoneda Dash nació en 2014, es calificada como una de las criptomonedas de la próxima generación. Fue creada por Evan Duffield (Arizona, 1980) quién también creó el algoritmo de minería X11. Al principio la moneda se llamaba Darkcoin pero por si la lección tuviera connotaciones negativas, se cambió el nombre a Dash, es un juego de palabras generado con la unión de “digital+cash”. Se considera que Dash mejora el sistema que aplica Bitcoin, tiene avances que mejoran el anonimato y la tecnología es más rápida al hacer transacciones.

Es una de las monedas que más usos ha encontrado en el mercado, cuenta con mecanismos de apoyo a los emprendedores y comisiones hasta doscientas veces más baratas que Bitcoin. Funciona con una red de dos niveles muy diferenciados. Uno de ellos es donde trabajan los mineros, quienes registran las transacciones y graban los bloques de la cadena. En el otro nivel están los llamados nodos maestros que se encargan de confirmar las transacciones y sostienen los servicios únicos de Dash. Ambos niveles son premiados por su trabajo, se divide la recompensa de la minería en tres partes, un 45% está destinado a los mineros, otro 45% es para los dueños nodos maestros y el 10% restante pertenece a la tesorería que da vida a la primera organización descentralizada autónoma totalmente exitosa en el mundo de las criptomonedas. Los nodos maestros tienen poder sobre la decisión de cómo invertir ese 10% de la tesorería. Dedican una parte de esa tesorería a la financiación o patrocinio de distintas actividades o personas, financiando a deportistas, becando a estudiantes, o financiando a emprendedores que lo solicitan así como proyectos educativos. Todo esto ayuda a que esta criptomoneda se extienda a una gran velocidad.

Observando la figura 10, que nos muestra la evolución del precio del Dash frente al euro desde su creación podemos ver que Dash en marzo del 2017 tenía un cambio de unos 90 euros, elevándose a gran velocidad, llego a los 180 euros en mayo y a los 360 euros en agosto. En noviembre del 2017 alcanzó su pico más alto llegando a un valor de unos 3.400 euros. Desde entonces ha mantenido una tendencia bajista hasta llegar al momento actual en el que su valor es de unos 67 euros.

Figura 10: Evolución del cambio dashs/euros desde su creación.

Fuente: https://www.coingecko.com/es/monedas/dash/eur

8.4 Ether

El desarrollo de la plataforma Ethereum[10] (ETH) en 2015 se debe al ruso Vitalik Buterin que trabajaba en ese momento en la tecnología de Bitcoin. Para su creación se utiliza la minería y su blockchain es programable lo que permite a los desarrolladores construir y desplegar aplicaciones descentralizadas y contratos inteligentes.

La moneda virtual se llama Ether que es un tocken que puede ser utilizado en las transacciones que utilicen la tecnología Ethereum. La finalidad de esta plataforma son los contratos inteligentes, que son una manera de garantizar que se cumplan unos acuerdos sin necesidad de que intervenga un tercero. Esta plataforma se encarga de ejecutar lo pactado cuando se cumplan las condiciones para ello. Es decir la manera de asegurarnos de que funcione X si se ejecuta Y. El ether, a diferencia del bitcoin, no tiene un número límite de monedas para su emisión. Si bien la creación de los tokens no fue inicia por etherum, en la actualidad existen más de 191.000 tokens etherum, considerándose con esa elevada cifra una de las criptomonedas que más tokens posee, cada uno de ellos con características únicas ejecutándose sobre su blockchain.

[10] Muchos más datos sobre esta criptomoneda pueden encontrase en Qué es Etereum (www.academy.bit2me.com)

La capacidad de Etherum para usar contratos inteligentes y construir tokens de forma sencilla ha llamado la atención de muchas empresas a nivel mundial, lo que ha logrado que distintas empresas creen la llamada Etherum Enterprise Alliance (EEA) que forman un conjunto de más de 100 miembros los cuales apoyan directa o indirectamente este tipo de tecnología. Entre estas empresas destacan: BBVA, Banco Santander, Cisco (empresa de redes más grande del mundo), JP Morgan (una de las más grandes firmas financieras del mundo), Microsoft (empresa de tecnología responsable del desarrollo de Windows) y otras muchas más.

Figura 11: Evolución del cambio ethers/euros desde su creación.

Fuente: https://btcdirect.eu/es-es/precio-ethereum

La figura 11 muestra la valoración de etherum en euros desde que esta moneda fue lanzada a la red. Tiene un cambio promedio de 187,65 euros con cambios volátiles muy similares a los sufridos por el resto de criptomonedas. Hay que destacar una gran bajada en junio del año 2017 debido a los rumores falsos sobre el fallecimiento de su creador y su rápida remontada una vez acallados esos rumores. Alcanzó su máximo histórico en enero del 2018, situándose en torno a los 1.250 euros.

8.5 Cardano

La plataforma Cardano[11] fue creada en 2015 por un grupo de inversores japoneses. El objetivo es conseguir la plataforma Blockchain más avanzada del momento. Se considera que constituye la tercera generación de criptomonedas, siendo bitcoin la primera y ether la segunda. Está tecnología está orientada a la investigación, elimina pequeños fallos que aún tienen otras criptomonedas, utiliza el nuevo lenguaje de programación Haskell que aporta un novedoso modelo de capas considerado mucho más seguro y fiable. Además, este lenguaje tiene capacidad para ser readaptado a medida que se considera necesario.

[11] Más información sobre Cardano puede encontrarse en Qué es Cardano? Qué es ADA? (www.cripto-mineria.com)

Se van a producir 45 billones de adas que son los tokens del cardano, frente a los 84 millones de litecoin y 21 millones de bitcoins. El trabajo de minería es diferente al utilizado con otras criptomonedas, en este caso se elige un minero al azar y este será el encargado de resolver el acertijo, no como en el resto que se lanza el acertijo a la red. Así se reduce el gasto energético en cuanto a minar. La tecnología Cardano pretende utilizar la tecnología Blockchain para llevar los sistemas bancarios a lugares donde antes era muy costoso implementarlos.

La figura 12 representa la evolución del precio en euros del Cardano desde su aparición. La moneda apareció oficialmente en los mercados de criptodivisas el 1 de octubre del 2017, con un valor aproximado de 0.018 euros y no fue hasta el 25 de noviembre cuando comenzó a incrementar su valor, creciendo un 300 por cien en un plazo de cuatro días y colocándose con un valor de 0.12 euros. Su máximo valor se dio en enero del 2018, que llegó a valer 1,19 euros. Actualmente su precio se ha recuperado tras la bajada que sufrió por el Covid-19. Su valoración general es escasa ya es un proyecto de reciente salida pero los expertos señalan que tiene grandes posibilidades.

Figura 12: Evolución del cambio cardanos/ euros desde su creación

Fuente: https://www.coingecko.com/es/monedas/cardano/eur

8.6 Stellar

La denominación Stellar[12] se refiere a una plataforma creada en el año 2016 para la transferencia de divisas normales aunque permite también transferencias de criptomonedas. La página www.bitcobie.com señala que la plataforma es bastante barata en las transacciones entre monedas ya que elimina muchas comisiones. Ripple y Stellar comparten fundador, pero Stellar es de código abierto sin ánimo de lucro, lo que no es el caso para Ripple.

Un activo esencial para el funcionamiento de la plataforma Stellar son los Lumens que son el sistema antispam para el bolckchain de la plataforma. Es una criptomoneda no minable, algo en lo que también coincide una vez más con Ripple, se crearon 100.000 millones de tokens. Un 95% de ellos se

[12] Más datos sobre la plataforma Stellar pueden encontrase en Qué es Stellar(XLM)? (www.academy.bit2me.com)

distribuyeron entre personas aleatorias titulares de bitcoins y ripples; el 5% restante se reservan para los costes operativos de la misma. Una transacción en esta red cuesta 0.0001 Lumens menos de 6 segundos, es decir prácticamente nada. Apunta a apoyar cualquier tipo de movimiento de divisas a personas que no pueden acceder, o no les resulta conveniente, a entidades financieras. A diferencia de otras criptomonedas, la finalidad de Stellar no es sustituir el dinero tradicional, sino que ambos convivan.

Como muestra la figura 13, su máximo histórico de 0,729104 euros se alcanzó en enero de 2018. Al igual que Cardano, o que otras muchas criptomonedas, es de reciente creación, por lo que aún necesita tiempo para observar una evolución más fiable.

Figura 13: Evolución de la valoración Stellar/ Euros desde su creación.

Fuente: https://www.coingecko.com/es/monedas/stellar

9. IMPACTO DE LAS CRIPTOMONEDAS

La creación de las criptomonedas está ligada a la evolución tecnológica ya que sin ella sería imposible considerar criptomonedas. La tecnología Bitcoin nunca hubiese sido posible sin todos los avances tecnológicos. Esta sección estudia los pros y los contras de la aparición de esta tecnología y cómo puede afectar a la sociedad.

Cualquier sistema financiero, por consolidado que esté, experimenta cambios necesarios con el transcurso del tiempo ya que se generan situaciones que hacen que la economía varíe enormemente y a gran velocidad. Precisamente la aparición de la crisis del 2008 abrió las puertas a un mundo desconocido para nosotros hasta el momento, se presentó el Bitcoin como una alternativa a la moneda tradicional que debido a la crisis financiera había sufrido devaluaciones. Este sistema digital presenta características en las que poder

salvaguardar capital y no sufrir de manera tan drástica las consecuencias que produce una situación de ese calibre.

Con la llegada de la tecnología Blockchain al mundo financiero la economía mundial comenzó a cambiar enfrentándose las divisas digitales al dinero tradicional y presentándose como la posible moneda del futuro.

Como hemos podido deducir a lo largo del trabajo observamos que el Bitcoin tiene características más y menos ventajosas, vamos a clasificarlas para mejorar su comprensión.

9.1 **Ventajas de las criptomonedas**

Una cuestión importante es lo relativo al poco tiempo que tardan en realizarse las transacciones con criptomonedas. Una transacción realizada con Bitcoin por ejemplo, es recibida pocos segundos después de realizarse y se empieza a confirmar unos diez minutos después. Este tiempo es el que hay que esperar para que la red confirme la operación para incluirla en un bloque dentro de la Blockchain antes de que los fondos puedan verse reflejados en su nuevo saldo. Las confirmaciones se crearon de tal manera que se duplican los tokens para pagar varias veces con los mismos y así evitar un doble gasto.

Con las criptomonedas se crea una nueva forma de cobro de comisiones. Las persona que realiza una operación de Bitcoin cuentan con la opción de colocar una comisión a la transacción que se entenderá como un incentivo para los mineros, por lo que serán las transacciones más rápidas, se pueden solicitar transacciones sin comisión pero no es lo más recomendable ya que el tiempo de espera será mucho mayor. Cuando realizamos una transacción, las carteras de criptomonedas nos recomiendan cuanto debería ser la cantidad que ofrezcamos de comisión para que se realice en un determinado tiempo promedio.

Otra cualidad que ha llamado mucho la atención de la sociedad es la privacidad. En la época tecnológica en la que nos encontramos el anonimato es casi impensable, no somos tan precavidos como cabría esperar, dejamos puertas abiertas continuamente ofreciendo muchísima información personal cada vez que abrimos un video, recibimos un correo, hacemos una compra o realizamos una búsqueda en internet. Esto es algo que hace unos pocos años nos aterrorizaría. Toda esta información es susceptible de ser hackeada, posteriormente vendida y utilizada para crear perfiles virtuales de cada persona, en ocasiones no es necesario ni que esta información se hackee ya que es entregada a los gobiernos de manera voluntaria. Tras entender hasta qué punto estamos expuestos podemos deducir que la actividad financiera de cada persona define dónde estás, que te gusta hacer, cuáles son tus debilidades, etc. Bitcoin lo que busca es que la privacidad sea garantizada para evitar que nadie pueda aprovecharse de los datos financieros personales y nadie sepa, si tú no quieres, en que gastas tu dinero. Aunque podemos

considerar el anonimato como un arma de doble filo, porque puede facilitar la economía sumergida, esto es una desventaja que estudiaremos más adelante.

Aunque las personas que realizan las operaciones cuentan con anonimato si así lo desean, estas operaciones quedan registradas en un libro contable descentralizado al que se puede acceder con libertad. Este libro contiene todos los movimientos, ya sean envíos o intercambios realizados dentro de la Blockchain de cada criptomoneda. Esto proporciona una garantía de la seguridad ya que este libro mayor resulta inviolable y también una clara transparencia ya que ofrece la posibilidad a cualquier persona pueda consultar los movimientos realizados en la blockchain.

Destacando la seguridad, las transacciones realizadas no se pueden revertir, solo pueden ser reembolsadas por las personas que reciben los pagos, la tecnología Bitcoin es capaz de detectar errores y no enviar transacciones erróneas o a direcciones no válidas.

En cuanto a su fiscalidad, no se aplica IVA (Impuesto sobre el valor añadido) en la transmisión de las monedas virtuales, es decir, la entrega de criptomonedas está exenta de IVA tanto para el comprador como para el vendedor de las mismas. Sólo se aplica el IVA en la compra de bienes o servicios, como si esta compra la realizásemos en euros. También está exenta la venta de Bitcoin por parte de entidades que se dedican al minado de la criptomoneda, aunque los mineros si están sujetos al IRPF (Impuesto sobre la renta de las personas físicas) o al IS (Impuesto de sociedades) si operan como sociedad.

Respecto al comercio exterior, podemos decir que las criptomonedas son las mayores aliadas de este tipo de comercio, facilitan las transacciones internacionales y elimina las comisiones en el giro de divisas que por lo general son elevadas, suelen ser porcentuales a la cantidad que se transfiere así que transferir grandes cantidades de divisas sale caro, las criptomonedas ponen solución a eso, es uno de los puntos que más popularidad las genera.

Las criptomonedas, aunque parezca que solo son para unos pocos expertos, no excluyen a nadie, permiten acceder a la red a una gran cantidad de personas que no tienen posibilidad de operar con bancos, ni la opción de tener tarjeta de crédito u otros medios de pago, gracias a las criptomonedas pueden operar solo teniendo a su disponibilidad internet.

9.2 **Desventajas de las criptomonedas**

Uno de los motivos por los que las criptomonedas han ganado tanta fama y se han colocado en el mercado de las inversiones tradicionales es la presencia de alta volatilidad. En el año 2018 el valor de la criptomoneda aumentó exponencialmente, eso llamo la atención de inversores en todo el mundo, sin embargo, dicha volatilidad se considera un arma de doble filo, ese mismo año el precio del Bitcoin perdió más del 50% de su valor, como consecuencia de eso el interés en el ámbito de las criptomonedas disminuye. Por eso se

requiere mucha valentía o tener un perfil de riesgo elevado para invertir en este mundo. Esta volatilidad se debe a varios factores, uno de ellos es la presencia de los medios, un rumor difundido a través de las redes sociales puede causar estragos en el valor de las criptomonedas, todo incidente que genere pánico en el público pone en peligro la estabilidad de los precios. Otro factor que influye en la volatilidad es lo que en el mundo de las monedas digitales denominan ballenas, esta denominación se refiere a aquellas personas que poseen una gran cantidad de Bitcon, esto se debe a que el Bitcoin sigue siendo pequeño en comparación con el resto del mundo de los activos, cuando estas personas realizan operaciones afectan a todo el mercado.

El mundo de las criptomonedas está creciendo, existen multitud de tipos de criptomonedas que han sido lanzadas en muy poco tiempo, esto genera incertidumbre sobre la elección de en qué moneda invertir, o que moneda llegará a ser más popular en el futuro y cual tendrá más valor. En realidad, con unos conocimientos adecuados cualquiera puede crear su propia criptomoneda.

El hecho de que las criptomonedas aún no hayan sido aceptadas globalmente es otro de los problemas al que se enfrentan. Algunos gobiernos están tomando determinadas medidas contra ellas pero otros gobiernos como puede ser el Chino están a punto de lanzar su propia criptomoneda. El 20 de junio del 2019 el Tribunal Supremo español se pronuncia por primera vez sobre el bitcoin, tras la sentencia nº326/2019 por la que se condena a alguien por un caso de estafa con Bitcoins. En esta ocasión, en lugar de devolver el dinero con el mismo medio de pago con el que se produjo la estafa, es decir Bitcoin, el tribunal consideró que se devolvería el valor en euros de cuando se produjo el delito, alegando que el Bitcoin no es dinero. Los gobiernos tienen motivos para no defender las monedas virtuales, la descentralización hace que se escapen de su control. Otro de los motivos que preocupa a los gobiernos es que las monedas virtuales pueden incentivar a mercados ilícitos.

Las criptomonedas están vinculadas con la compra de mercancía ilícita en el llamado internet profundo. En 2019 se desmantelo una red de pederastas que operaban con Bitcoins en más de 28 países y a pesar de que se endurece día a día la reglamentación de las monedas virtuales, las actividades ilegales aun no pueden resolverse. El anonimato ofrece a los posibles criminales una seguridad para poder llevar a cabo sus actividades delictivas que no encuentran con la utilización de las monedas fiduciarias. En 2014 se lanzó una criptomoneda llamada Monero, es una de las más utilizada en la web oscura, aunque su capitalización es mucho menor que la de Bitcoin, utiliza una arquitectura muy compleja que hace difícil rastrear las transacciones, por eso es la más utilizada por este tipo de usuarios.

Las plataformas que permiten la adquisición y venta de criptomonedas, llamadas Exchange, han sufrido robos multimillonarios. A pesar de que se invierte mucho dinero en seguridad para evitar el robo de activos, esto no hace que sean inquebrantables. Durante décadas, las entidades bancarias han mejorado de manera constante sus sistemas de seguridad y aun así sufren

robos no solo presenciales, si no también mediante las aplicaciones de banca electrónica, Bitcoin tiene apenas 12 años, es obvio que aún le queda camino por recorrer en este ámbito y mucho trabajo para hacer cada vez un sistema más seguro. El método más utilizado hasta el momento para realizar las sustracciones de fondos[13] está detrás de esquemas piramidales conocidos como esquemas Ponzi[14].

El hecho de que las operaciones realizadas con monedas virtuales sean irreversibles es fundamental para la seguridad de su sistema, pero tiene una clara parte negativa, en el caso de cometer un error al realizar alguna operación está será irreversible, por lo que se perderían los activos.

Por último, se aborda el impacto social que generan las criptomonedas. Digitalizar el dinero supondría el aislamiento de personas desfavorecidas sin facilidad de acceso a internet o a un móvil y también la dificultad que crearía entre las personas mayores que no están acostumbradas a la tecnología.

Por otro lado, todas las personas que trabajan en la economía sumergida y cobran un sueldo en efectivo, sin contrato, muchos de ellos por no tener los papeles en regla, no podrían seguir con esta práctica, lo que podría suponer o bien un aumento de la delincuencia, o frenar la inmigración ilegal, o que se vuelva a prácticas ya eliminadas hace siglos como el trueque, etc.

Otro aspecto es el consumo energético del movimiento y creación de criptomonedas lo que supone un duro golpe para la economía verde.

9.3 **A favor y en contra: la descentralización**

Otra característica necesaria de ser analizada es la descentralización que es posiblemente la más importante de las características de las monedas virtuales. Esta característica tiene su parte positiva y su parte negativa. La red Bitcoin como ya hemos estudiado está formada por nodos como las redes p2p, esto quiere decir que no existe un servidor central o una unidad única de la que

[13]Silk Road era una conocida tienda de la web oscura, donde se podía comerciar con mercancía ilegal. El FBI consiguió clausurar este mercado ilegal, durante los trabajos de detención se incautaron 29.655 bitcoins propiedad de esta tienda individual y 144.000 Bitcoins propiedad del fundador del sitio web, por lo que este caso puede catalogarse de robo o de justicia. Otra de las mayores Exchange de la historia, es Bitfinex, con sede en Hong Kong y fundada en el año 2012, esta empresa ha sido víctima de dos robos importantes, el primero en 2015 donde se robaron unos 1.500 bitcoins y el segundo mucho más importante en Agosto del año 2016, en el que mediante una brecha de seguridad sustrajeron 119.756 bitcoins; a día de hoy la empresa continua operativa y, en este caso, los usuarios si recuperaron sus bitcoins. Hay muchos más robos de monedas virtuales cada año, por lo que está claro que los sistemas no son totalmente seguros.

[14] Reciben su nombre de Charles Ponzi, un italiano que puso en práctica este tipo de fraude en Boston, en los años 20 del siglo pasado, finalmente fue detenido por haber hecho quebrar a varios bancos y arruinado a miles de inversores; este sistema es un montaje financiero fraudulento en el que se garantizan intereses a los inversores que se pagan gracias a los fondos aportados por nuevos inversores, lo que significa que los últimos en entrar en el sistema siempre pierden.

dependa la red. La gran ventaja es que existe más seguridad al no depender de un solo servidor. En cuanto a su valoración, el hecho de que esté descentralizada, significa que ninguna entidad la respalda, por lo que depende completamente de aquellos que operen con ella. Este hecho supone que no afecte necesariamente a su valoración sobre el resto de los mercados, pero también que no exista ningún respaldo.

10. CONCLUSIONES

Estos últimos años estamos siendo testigos de un camino incierto, con una constante velocidad en la innovación. A costa de esto nos resulta difícil imaginar cómo evolucionará nuestro modo de vida con el paso del tiempo, qué puestos de trabajo serán creados, qué tipo de industria prevalecerá, cómo avanzará la comunicación, la formación, y un sinfín de conceptos. Toda esta incertidumbre genera dudas y miedos lógicos ante lo poco conocido. Sin embargo, todos tendremos que adaptarnos, pues el cambio es innegable y acaba de empezar.

Para concluir el trabajo se quiere destacar seis aspectos de las criptomonedas que agregan, de alguna forma, la innovación que representan aunque no significa una valoración positiva pues en muchas ocasiones contienen elementos de ventaja y desventaja.

- Descentralización: las monedas no están controladas por ninguna autoridad, quedan fuera sus transacciones del pago de impuestos.
- Anonimato: aunque cada operación que se realiza en la red queda registrada, su dirección no está vinculada a ninguna persona en particular y de este modo se asegura el anonimato. No obstante, puede potenciar el blanqueo de capital y utilizarse de manera ilícita.
- Flexible: se puede crear fácilmente sin que suponga ningún coste de apertura o comisión, además elimina las barreras transfronterizas y no exigen requisitos para su obtención o trasferencia.
- Rápido, se envían las transacciones en cuestión de segundos confirmándose en muy pocos segundos las transferencias.
- Tarifas de transiciones baratas, actualmente la trasferencia de bitcoins es gratuita, pero contamos con la opción de pagar una comisión y que se realice de manera automática, esto terminará siendo un incentivo para los mineros cuando se termine la emisión de las monedas.
- Volatilidad: la valoración de las criptomonedas en general y del bitcoin en particular fluctúan de manera muy palpable, por lo que es muy difícil adelantarse a sus valoraciones en el tiempo.

BIBLIOGRAFÍA

Ammous, F. (2019). El patrón bitcoin: la alternativa descentralizada a los bancos centrales. Ed. Deusto

Assange, J., Appelbaum, J., Müller-Maguhn, A. y J. Zimmermann. (2012). Cypherpunks: freedom and the future of internet . OR Books. London-NewYork.

BBVA.com. Historia de las tarjetas de crédito. Consultado en julio de 2020.

Brito, J. y A. Castillo. (2013). Bitcoin: A Primer for Policymakers. Research Gate.

Calvo, M. (2018). "Conoce los diferentes tipos de blockchain." Obtenido de Blockchain Services: http://bit.ly/2FpKk4C

CriptoNoticias. (2018) "¿Cómo elegir un monedero de bitcoin y otras criptomonedas?" Disponible en: http://bit.ly/2vfeWAo

Disanzo, M. (2006). Redes Peer-to-Peer y Tecnología JXTA. Disponible en www.dsi.fceia.unr.edu.ar

European Banking Authority. (2014). EBA Opinion on 'virtual currencies' (eba.europe.eu).

European Central Bank- Eurosystem. (2012). Virtual currency schemes. (Version online). Frankfurt.

Gates, M. (2017). Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. CreateSpace Independent Publishing Platform.

Hernández, L. (2016). La criptografía. Ed. Consejo Superior de Investigaciones Científicas. Madrid.

Herrera, C. (2018). "¿Qué son los contratos inteligentes o Smart Contracts?" Tekcripy

Miller, M. (2014). The ultimate guide to Bitcoin. Pearson Education. Indiana.

Satoshi Nakamoto. (2008). Bitcoin: un sistema de dinero en efectivo electrónico peer- to- peer. Artículo libre en red sathosin@gmx.com. www.bitcoin.org.

Schueffel, P., Groeneweg, N. y R. Baldeggerl. The crypto encyclopedia: coins, tokens and digital assets from A to Z. (2019). Global Books. Bern, Switzerland.

Valoración del precio del Bitcoin (consultado en Mayo y Junio) disponible en: https://btcdirect.eu/es-es/precio-bitcoin

Valoración del precio del Litecoin (consultado en Mayo y Junio) disponible en: https://btcdirect.eu/es-es/precio-litecoin

Valoración del precio del Ripple (consultado en Mayo y Junio) disponible en: https://btcdirect.eu/es-es/precio-ripple

Valoración del precio del Dash (consultado en Mayo y Junio) disponible en: https://www.coingecko.com/es/monedas/dash/eur

Valoración del precio del Etherum (consultado en Mayo y Junio) disponible en: https://btcdirect.eu/es-es/precio-ethereum

Valoración del precio del Cardano (consultado en Mayo y Junio) disponible en: https://www.coingecko.com/es/monedas/cardano/eur

Valoración del precio de Stellar (consultado en Mayo y Junio) disponible en: https://www.coingecko.com/es/monedas/stellar

Vanci, M. (2020) "Bitcoin resiste la crisis económica por coronavirus y hasta se fortalece, según análisis". Disponible en: Criptonoticias.com

Zamorano, V. "¿Quiénes son los cypherpunks?" (2018) http://www.blockchainservices.es/uncategorized/