FACULTAD DE TURISMO Y FINANZAS

GRADO EN FINANZAS Y CONTABILIDAD

Análisis y Evolución de una Criptomoneda: El Bitcoin

Trabajo Fin de Grado presentado por Rocío González Medina, siendo la tutora del mismo la profesora Dolores Gómez Domínguez

Vº. Bº. Dolores Gómez Domínguez

Rocío González Medina

D. /Dña. Dolores Gómez Domínguez

D. /Dña. Rocío González Medina

Sevilla junio de 2019

GRADO EN FINANZAS Y CONTABILIDAD

FACULTAD DE TURISMO Y FINANZAS

TRABAJO FIN DE GRADO

CURSO ACADÉMICO [2018-2019]

TÍTULO:

ANÁLISIS Y EVOLUCIÓN DE UNA CRIPTOMONEDA: EL BITCOIN

AUTOR:

ROCIO GONZALEZ MEDINA

TUTOR:

Dra. Dª DOLORES GÓMEZ DOMÍNGUEZ

DEPARTAMENTO:

ECONOMÍA APLICADA III

ÁREA DE CONOCIMIENTO:

MÉTODOS CUANTITATIVOS PARA LA ECONOMÍA Y EMPRESA

RESUMEN:

Bitcoin es una moneda virtual que ha adquirido importancia estos últimos años. Se caracteriza por no tener representación física, por ser global y descentralizada. Estas cualidades han dado a Bitcoin popularidad. También son la causa de las ventajas e inconvenientes que este valor plantea

Uno de los aspectos destacado de esta criptomoneda es su alta volatilidad.

El sistema que usa Bitcoin se llama peer-to-peer y su emisión se realiza mediante un proceso de minería. Bitcoin se encuentra protegido por un sistema de seguridad llamada criptografía.

El objetivo del trabajo es explicar qué es el Bitcoin, cuál fue su origen y que evolución han tenido las principales magnitudes de esta divisa: usuarios, transacciones, capitalización del valor y cotización en el mercado de divisas. Concluimos con un ejemplo para estudiar si hay arbitraje entre Bitcoin, Dólar y Euro.

PALABRAS CLAVE:

Criptomonedas; Bitcoin; Peer-to-peer; Sistemas de pagos; Blockchain

ÍNDICE

CAPÍTULO 1 INTRODUCCIÓN

1.1 INTRODUCCIÓN

Los avances tecnológicos, el que cada día se cuente con equipos informáticos más potentes y el desarrollo de nuevas herramientas de computación, han hecho que aparezcan nuevos medios que facilitan el intercambio y nuevos mecanismos de pago.

El dinero de "plástico", que es como se denomina coloquialmente a las tarjetas de crédito, apareció hace ya unas décadas, pero su uso generalizado es más reciente. La primera tarjeta que permite el pago en varios establecimientos se crea en 1949. En la década de los 50 del pasado siglo surgen dos de las tarjetas más populares, Bank Americard (VISA) y Interbank Card Association (MASTERCARD)[1]. En España, la introducción de las tarjetas es posterior, concretamente en la década de los setenta, extendiéndose su uso a partir de la década de los 90 del pasado siglo (Marín López, 2004).

El dinero electrónico es, en sentido amplio, cualquier medio de pago que requiera del uso de tecnología electrónica. En un sentido más restringido, como recoge el Banco de España, en el portal del cliente bancario, el dinero electrónico consiste en almacenar dinero que está físicamente en billetes y monedas, en una cuenta corriente o en una tarjeta de crédito, en cualquier soporte electrónico como puede ser una tarjeta física, una tarjeta virtual, un teléfono, un ordenador o cualquier otro dispositivo cuya memoria permita hacerlo, que luego puedes utilizar para realizar pagos con el límite del importe que hayas cargado[2]. En este sentido más restringuido, no se incluiría en la categoría de dinero electrónico algunas de las formas de pago que actualmente existen. Sólo aquellas que tienen detrás el respaldo de efectivo denominado en una moneda de curso legal. El origen del dinero electrónico, según Espinach y Ruzicka (1999), se produce en 1972 mediante la creación de una red que permite la transferencia entre la matriz del Banco de la Reserva Federal de San Francisco y sus filiales.

En todos estos casos estamos hablando de dinero, es decir, un bien o activo aceptado como medio de pago o medición de valor por los agentes económicos para sus intercambios y que actúa como unidad de cuenta y depósito de valor.

Sin embargo, más recientemente, aparecen otros instrumentos que tienen como objetivo ser una herramienta para el intercambio, se trata de las denominadas criptomonedas, un tipo de moneda virtual descentralizada que utiliza claves criptográficas para su generación. La primera de este tipo de monedas es el Bitcoin cuyo origen se remonta al año 2008 (Nakamoto, 2008)[3]. Existen monedas virtuales privadas con origen anterior (Down, 2014) siendo quizás la más conocida e-gold.

Coincidiendo con la desaparición de e-gold y en plena crisis financiera internacional se crea una nueva divisa virtual, denominada bitcoin, que utiliza la criptografía para la creación y transferencia de la moneda. Este trabajo se detiene fundamentalmente en

[1] Existen incluso referencias a la creación de tarjetas que sitúan su origen en la segunda década del siglo XX (BBVA, s.f.).

[2] Portalclientebancario, Banco de España. En https://clientebancario.bde.es/pcb/es/menu-horizontal/productosservici/serviciospago/Dinero_electronico.html, consultado 01/03/2019

[3] En este trabajo se plasma el proyecto, aunque la primera unidad se generó en 2009.

el análisis de las monedas virtuales del tipo criptomonedas y más concretamente en la pionera y de mayor popularidad y uso, el bitcoin.

Para ello el estudio se estructura como sigue. En el capítulo 2 nos centramos en el auge de los pagos digitales, es decir, la sustitución creciente para las transacciones de esta forma de pago frente al tradicional pago en efectivo. Sin que se hubiera producido este fenómeno, que va unido al del auge del comienzo electrónico, hubiera sido difícil conseguir éxito en el lanzamiento de las criptomonedas. Aunque entre los argumentos de los defensores de este nuevo medio de intercambio está la seguridad, la agilidad y los menores costes de transacción, el objetivo principal que persiguen las criptomonedas es disponer de un medio de pago global que no esté bajo el control de una autoridad monetaria central.

En el capítulo 3, se aborda el origen del bitcoin, su definición y características básicas. Hay que tener en cuenta que en la actualizada funciona 2177 criptomonedas con una capitalización de mercado de 237.522 millones de dólares. Sin embargo, de esa capitalización más de 142.251 millones de dólares, es decir, cerca del 60% corresponde a Bitcoin[4].

Aunque sus orígenes se remontan a 2009, y fue revolucionaría la tecnología incorporada en su creación, la de los registros distribuidos, por la seguridad y anonimato que proporcionaba, el auge de la divisa en cuanto a utilización en las transacciones y en su cotización comienza a producirse a partir del año 2013. Unido a ese auge aparecen las opiniones de defensores que realzan sus ventajas y detractores que señalan sus inconvenientes. Es también a partir de este momento cuando la divisa atrae la atención de reguladores y distintos organismos[5] que hasta el momento analizan su función como medio de intercambio sin aceptarla como medio legal de pago[6]. Una síntesis de las ventajas e inconvenientes se recoge en el capítulo 4.

En el capítulo 5 se presenta la evolución de las principales magnitudes del bitcoin, número de unidades emitidas, capitalización del mercado, transacciones realizadas y cotización. Cerramos el capítulo con un ejercicio para poner de manifiesto la posibilidad de arbitraje y especulación.

Finalmente, en el capítulo 6 se recogen, a modo de conclusión, un conjunto de reflexiones finales. El trabajo se cierra con las referencias bibliográficas y un anexo con un glosario de términos.

Para la elaboración de este trabajo no hemos apoyado en fuentes bibliográficas, páginas web de entidades públicas y privadas y hemos utilizado la hoja de cálculo Excel 2016 para el ejercicio recogido en el capítulo 5.

[4] Según aparece en la página coinmarket, https://coinmarketcap.com/es/ (consultado 17 de mayo de 2019)

[5] En nuestro entorno destacan los informes de la Autoridad Bancaria Europea (2014) y Banco Central Europeo (2012).

[6] La controversia sobre si se trata de un medio intercambio o un medio de pago es abordada por Nieto Giménez-Montesinos y Hernáez Molera (2018) destacando que la admisión de la divisa como medio de pago requeriría la autorización previa para su emisión.

CAPÍTULO 2: SISTEMAS DE PAGOS ELECTRÓNICOS, MONEDAS VIRTUALES Y CRIPTOMONEDAS

Como hemos indicado en la introducción, los avances tecnológicos han permitido la aparición de medios de pagos distintos de los tradicionales.

En nuestra vida cotidiana traspasamos o transferimos dinero de una cuenta bancaria a otra sin que el efectivo pase por nuestras manos. De igual forma al pagar en cualquier establecimiento en lugar de utilizar efectivo utilizamos una tarjeta de "plástico" o el móvil y cuando compramos por internet introducimos unas claves que facilita una entidad bancaria y que da acceso a una pasarela de pago. Pero comúnmente, aunque sea mediante un medio electrónico, la mayoría de las operaciones se realizan denominadas en algunas de las monedas de curso legal.

También se podría utilizar para pagar un sistema de claves vinculado a una moneda virtual, si disponemos de ella, y es aceptada como medio de intercambio o de pago.

2.1 DINERO VIRTUAL, MONEDAS VIRTUALES Y CRIPTOMONEDAS

En la actualidad, podemos afirmar que el denominado dinero digital ha ido desbancando al efectivo. La mayoría de las transacciones hoy en día se hacen de forma digital. Cuando usamos la terminología "dinero digital" hacemos alusión a todo tipo de intercambio que se lleve a cabo mediante un medio electrónico.

Un ejemplo que se usa en la vida cotidiana es la transferencia, que consiste en pasar dinero de una cuenta a otra, el dinero que se traspasa es dinero digital. Otro ejemplo que se utiliza en el día a día y que no se suele ser conscientes de ello son las tarjetas, cuando nos servimos de ellas para pagar en los comercios.

Podemos concluir lo expuesto anteriormente enunciando que todo pago o envío de dinero que se lleve a cabo sin usar para ello dinero físico, se lleva a cabo con dinero digital.

Por otro lado, encontramos la moneda virtual, que solo existe en formato digital y que no tiene formato físico. En la actualidad hay numerosos videojuegos que tienen su propia moneda virtual para adquirir objetos, normalmente también virtuales, o fases del juego. Un ejemplo de gran popularidad sería los "paVos" que son la moneda virtual del videojuego Fortnite de Epic Games[7]. También habría que incluir los puntos de fidelización, que nos otorgan ciertos establecimientos y que podemos canjear por productos o servicios. Sin embargo, se trataría de monedas de red cerrada que sólo se pueden utilizar en un determinado entorno, ya sea el videojuego o el comercio o conjunto de comercios que otorgan los puntos.

Con lo enunciado en el párrafo anterior no se quiere expresar que todas las monedas virtuales se utilicen sólo en los circuitos de los videojuegos o sean monedas de red cerrada, pues encontramos otras divisas que fueron creadas por entidades empresariales o simplemente por aficionados, con el objetivo de competir o reemplazar a las monedas de curso legal vigentes por una moneda nueva que no está bajo el control de una autoridad monetaria

Analizando la definición de moneda virtual se saca en conclusión que todas las monedas virtuales son digitales, puesto que no hay un formato físico de ellas. De este concepto surge la frase "toda moneda virtual es digital, pero no todo el dinero digital es

[7] Se puede conseguir superando fases del juego o bien comprándola.

virtual", por ejemplo, una cuenta bancaria denominada en moneda euro es digital, pero, por el contrario, no es virtual.

En Nieto Giménez-Montesinos y Hernáez Molera (2018) se definen las criptomonedas como monedas virtuales, descentralizadas y que no poseen un emisor concreto. El tipo de criptomoneda más conocido es el Bitcoin que usa la tecnología DLT (Distributed Ledger Technology), gracias a ella se puede ver el historial de las operaciones ejecutadas. Existe una base de datos, que la tiene todos los usuarios en la que se registra las operaciones y los mineros se encargan de verificarlas.

Para el Banco Central Europeo, tal y como recoge en su página web refiriéndose a la criptomoneda Bitcoin, se trata de una unidad de valor digital que puede ser intercambiada electrónicamente, pero no se trata de una moneda. Para esta institución, se trata de un medio de intercambio electrónico sin respaldo, es decir nadie garantiza su derecho a usarlo, ni trabaja para mantener su valor. Tampoco es un medio de pago generalmente aceptado y es tremendamente volátil. Concluyen, señalando que se trata de un activo especulativo y, por tanto, de gran riesgo que se acentúa en ausencia de regulación.

Las criptomonedas estas caracterizadas por:

- No poseer representación física
- Ser descentralizadas
- Ser globales

El 22 de mayo de 2010 fue el día que se realizó por primera vez una transacción con Bitcoin. El señor Laszlo Hanyecz, un programador de procedencia estadounidense, adquirió un par de pizzas cuyo valor ascendió a 10.000 Bitcoin, que en aquel momento equivalía a unos 30 euros[8] . Si se utiliza la cotización promedio de abril de este año, 4.588,3 euros por Bitcoin[9], y el que vendió las pizzas hubiera conservado el Bitcoin tendría 45.883.000 euros.

2.2 SISTEMAS DE PAGOS ELECTRÓNICO

Los sistemas de pagos electrónicos se utilizan en las compra-ventas electrónicas en las que el comprador necesita transferir dinero al vendedor de forma digital, por lo que el dinero electrónico adquiere una de gran relevancia a la hora de realizar una compra-venta en un comercio electrónico, un ejemplo de ello es Aliexpress.

En la figura 2.1 se recoge la evolución experimentada por los distintos métodos de pagos utilizados en las compras online en los años 2015, 2016 y 2017.

[8] Así lo recoge Sandra Pérez en un artículo de la Revista Fortune, con el título "La primera transacción fue para comprar pizza", en https://www.fortuneenespanol.com/tecnologia/historia-bitcoin-pizza-day-blockchain/ consultado 06/04/2019

[9] Dato tomado de investing.con, en https://es.investing.com/crypto/bitcoin/btc-eur-historical-data, consultado el 2/05/2019.

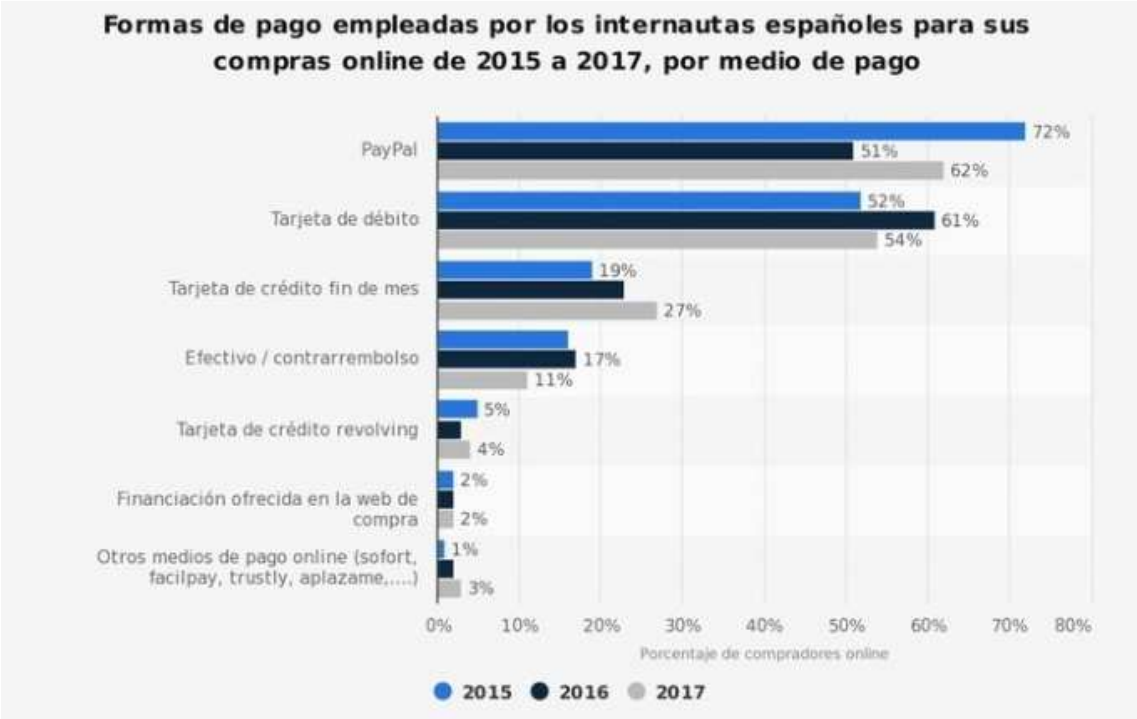


Figura 2.1 Diferentes formas de pagos con un medio electrónico

Fuente: El Observatorio Cetelem; CanalSondeo, INE (Spain)[10]

Como se observa, el primer lugar lo ostenta Paypal[11], cuyo éxito radica en que, además de ofrecer un servicio de pago seguro en la red, actúa como mediador entre comprador y vendedor si se produce una reclamación. El usuario a través de su cuenta Paypal o bien con una cuenta bancaria puede ejecutar el pago. Como desventajas se destaca su coste, que es un poco elevado, pues el usuario deberá asumir un pago mínimo de 0,35€ + el 3,5% por transacción.

El segundo lugar lo ocupan las tarjetas bancarias, las más usadas son Visa y MasterCard. Gracias a ellas se tiene acceso al 90% de las ventas que se producen por TPV.

Como podemos observar en la gráfica, Paypal sufrió una caída en porcentaje de uso como medio de pago online de 2015 a 2016, se recuperó en 2017 aunque sin alcanzar el porcentaje de 2015, pues se quedó 10 puntos porcentuales por debajo. Las tarjetas bancarias, por el contrario, han ido ganando cuota pasando de un 52% a un 54% y de un 19% a un 27%.

Muchos menos peso tienen el efectivo, las tarjetas de crédito revolving, la financiación ofrecida a través de la web y otros medios de pagos, con una representación minúscula.

Seguidamente, en las figuras 2.2 y 2.3 se recoge la evolución seguida por las operaciones realizadas con tarjeta en el periodo 2002-2014, en número de operaciones y en importe, respectivamente.

[10] https://youneselazizi.com/metodo-pago-comercio-electronico/ Consultado 3/04/2019

[11] Plataforma de pagos que funciona como una billetera electrónica.

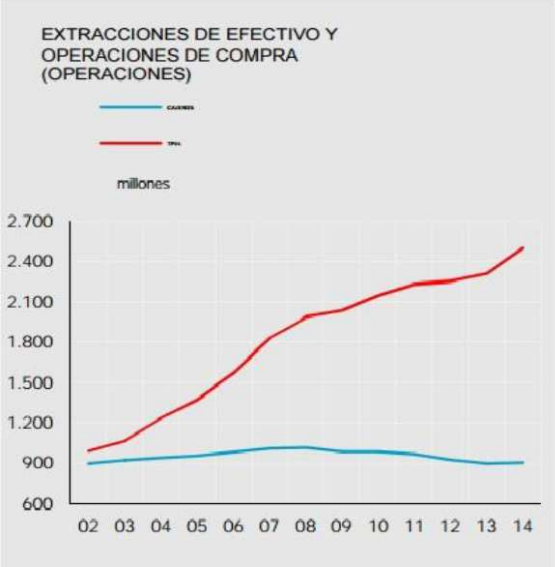


Figura 2.2: Operaciones cajero y tarjeta

Fuente: Banco de España

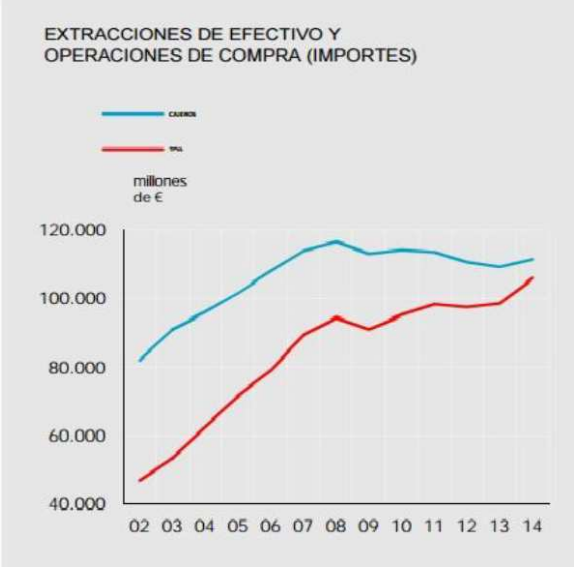


Figura 2.3: Dinero en metálico vs virtual

Fuente: Banco de España

En la figura 2.2 y figura 2.3 aparecen representada dos líneas. La línea azul hace referencia a las extracciones de dinero que se realizan y la línea roja, representa las operaciones que se han realizado con tarjera de crédito.

En el primer trimestre de 2016 el Banco de España aprecio por primera vez como la cantidad de dinero gastada con tarjeta (27.816 millones de euros) era superior a la retirada en efectivo (26.603 millones de euros).

Con el paso del tiempo el dinero de plástico ha sustituido al dinero en efectivo. Este movimiento se ha producido en parte por las comisiones que cobraban los bancos por retirar efectivo de sus cajeros sin ser clientes. Un ejemplo de ello nos los muestras Urrutia (2016) en un artículo publicado en el periódico El Mundo[12].En dicho artículo, se pone como ejemplo, el caso de Caixabank que a principios de 2016 comenzó a cobrar una comisión cercana a dos euros en las operaciones de retirada de efectivo de sus cajeros con tarjetas que no eran de su red.

Otro motivo que ha contribuido a dicho cambio ha sido el interés de las entidades financiera en que los usuarios usaran las tarjeras. En el año 2015, se retiró de los cajeros 114.862 millones de euros, lo que requirió un coste de 112.330 millones de euros en concepto de puesta en marcha de cajeros, seguridad, mantenimiento y otros costes derivados de dicha actividad. Este coste fue cubierto por las comisiones que se cobraron a los clientes.

En la página web del Banco Central Europeo[13] podemos ver el porcentaje de sucursales clausuradas desde la crisis, dicho número se eleva a un 32%, es decir, unas 14.978 sucursales. Si los comparamos con el número de cajeros eliminados, la diferencia es de 14%, pues el número de cajeros automáticos que se suprimieron fue de 50.335 cajeros, es decir, un 18%.

Previsiblemente, en el futuro, el dinero electrónico se usará más que el dinero en efectivo. Debido al desarrollo de la tecnología la forma de pago tradicional está

[12] Urrutia (2016) Las compras con tarjeta superan por primera vez a las de efectivo. *El mundo.* https://www.elmundo.es/economia/2016/07/02/5776c55d22601d4a2d8b45d1.html

[13] https://www.ecb.europa.eu/ecb/html/index.es.html Banco Central Europeo consultado 16/04/2019

disminuyendo, aunque el dinero en papel no desaparecerá por completo, el dinero digital irá ganando terreno (Jiménez y Tejero, 2018).

No obstante, parece que, a día de hoy, todavía es necesaria la intervención de las entidades financieras en su papel de intermediación en este tipo de operaciones. Los usuarios no tienen la suficiente confianza en este tipo de operaciones, por ello es necesario la presencia de dichas entidades que aporten un grado de seguridad y que permitan que los usuarios confíen.

En el artículo previamente citado Urrutia (2016), se propone una solución, la cual incluye un sistema de pago con pruebas criptográficas seguras que hace que se incremente la confianza de los usuarios y elimine la presencia de terceros. Este sistema de criptografía, que posee la mayoría de las criptomonedas supone un avance tecnológico importante.

2.3 TIPOS DE CRIPTOMONEDAS

En el trabajo de Plassaras (2013) y en el artículo de Monzón (2019), entre otros, se destaca el Bitcoin como eje principal para poder entender su funcionamiento, ventajas, características… El Bitcoin tiene tanta importancia porque fue la primera moneda en crearse.

Hoy en día existen una gran variedad de criptomonedas. Según se recoge en el portal de internet coinmarketcap, especializado en proporcionar información sobre divisas digitales, existen en el mercado 2177 criptomonedas[14] . A continuación, en la tabla 2.1 se muestra varios tipos de criptomonedas ordenadas de mayor a menor nivel de capitalización de mercado.

Nombre	Año de	Precio[15]	Capitalización de	Unidades en

[14] https://coinmarketcap.com, consultada el 17/5/2019.

[15] Los valores del precio, capitalización del mercado y acciones en circulación fueron rescatado de la página Coinmarket, el día 18/05/2019, actualmente dichos valores pueden oscilar como consecuencia de las fluctuaciones del mercado https://coinmarketcap.com/

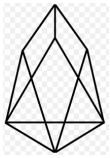
	Creación		Mercado	circulación
Bitcoin BTC 	03/09/2009	7.314,01 USD	129.577.081.382 USD	17.707.887 BTC
Ethereum ETH 	30/07/2014	237,07 USD	25.158.589.050 USD	106.121.599 ETH
Ripple XRP 	09/2012	0,374093USD	17.119.551.323 USD	42.133.310.721 XRP
Bitcoin Cash BCH 	01/09/2017	361,80USD	7.39.775.494 USD	17.790.988 BCH
Litecoin LTC 	07/10/2011	94,97 USD	5.873.047.111 USD	61.843.876 LTC
EOS.IS EOS 	06/2017	5,93 USD	5.760.007.785 USD	912.280.408 EOS

Tabla 2.1 Diferentes tipos de Criptomoneda

Fuente: Elaboración propia a partir de los datos contenidos en coinmarketcap.com

CAPÍTULO 3: LAS CRIPTOMONEDAS: ¿EL DINERO DEL FUTURO?

Como hemos señalado en el capítulo anterior, la primera criptomoneda y de mayor popularidad es el Bitcoin. A continuación, trataremos los aspectos básicos de la misma, empezando por su definición y características. Concluiremos el capítulo con algunas otras criptomonedas relevantes que han aparecido después del Bitcoin.

3.1 DEFINICIÓN Y ORIGEN DEL BITCOIN

3.1.1 Definición de Bitcoin

Según Vásquez Leiva (2014), el Bitcoin es un medio de intercambio electrónico, que se sirve de un protocolo y una red computacional.

Sin embargo, The Bitcoin Foundation nos aporta otra definición: con Bitcoin encontramos un nuevo sistema de pago y una moneda digital 100%. Bitcoin es una red consensuada, además es una red pionera que acepta el pago entre pares, es decir, de comprador a vendedor sin intermediario de por medio, descentralizado e impulsado por los usuarios. No cuenta con una autoridad central. Para el usuario, Bitcoin es como dinero para Internet. Además, es un sistema de contabilidad triple.

Las dos definiciones anteriores llevan a preguntarse ¿se trata de una red que permite efectuar pagos o se trata de una moneda para realizar intercambio? La respuesta es que ambas. Seguidamente se plantea un ejemplo para poder explicarlo.

Imaginemos que se quiere adquirir un estuche, por lo que se plantea dos opciones, la primera es ir a una tienda y hacer un intercambio del estuche por una cantidad de monedas, la segunda opción que se plantea es adquirirlo a través de la red, es decir, se produce un intercambio al igual que se ha producido en la primera opción, pero con la salvedad de que al dueño no se le ve físicamente. Si optamos por la segunda opción tenemos que hacer uso de una plataforma para verificar que los datos son correctos antes de efectuar el pago.

Sirviéndonos del ejemplo que hemos planteado anteriormente para definir Bitcoin, se enuncia que la red Bitcoin es una plataforma diseñada para utilizar la moneda Bitcoin, que posee una serie de normas. La red encripta las operaciones para proporcionar seguridad. Se trata de una red desarrollada por los usuarios y su canal de distribución es internet, que permite realizar pagos y verificar las transacciones en tiempo real con poco coste.

A continuación, se trata la parte de la definición que hace referencia a Bitcoin como un sistema de contabilidad triple.

En primer lugar, se explica que quiere decir eso. Actualmente el control de las operaciones financiera que se realizan en las entidades tanto públicas como privadas se lleva mediante un sistema de contabilidad denominado “la partida doble”, cuyo nacimiento se le atribuye al fraile franciscano Luca Pacioli en el siglo XV (Smith, 2009). Este sistema consiste en establecer registros contables tanto en el debe como en el haber del libro de cuentas.

El sistema de contabilidad triple consiste en la recogida de apuntes contables en el debe y en el haber como en el sistema doble y en un tercer asiento. Arjona (2013), nos explica como la tercera partida muestra y valora el importe que modifica los movimientos de flujos de fondos, viéndose alterado, como consecuencia, el estado de flujos de efectivo. De esta forma, en el asiento de la contabilidad triangular, no solo se coordinan las dos partes esenciales de un hecho contable: la primera conocida como

origen o fuente de financiación, que se ve reflejada en el haber, y la segunda que hace referencia a un fin o inversión, que la podemos encontrar en el debe, sino que añade una tercera parte, la cual se conoce como el movimiento de flujo de efectivo (que no caja).

La contabilidad triangular posee un doble propósito: por un lado, se hace presente el flujo en la misma operación que registra el asiento contable, y, por otro lado, facilita la elaboración del estado de flujo de efectivo por la suma del saldo de las cuentas, proporcionando un mayor control de las operaciones realizadas con Bitcoin ya que refleja el movimiento de los flujos y aporta información útil y valiosa.

Los comentarios en cuanto a la definición de bitcoin de los expertos son diversos.

Mar Galtés (2013), redactora de economía del periódico La Vanguardia define el Bitcoin como uno de los tantos sistemas de pago cuya función es convertir el dinero físico en bytes. La diferencia de Bitcoin con otros sistemas es que no posee ninguna entidad que afirme la autenticidad del dinero que se intercambia, es decir, no hay un Banco Central de Bitcoin que emita o regule dicha divisa.

En el mismo artículo se ven reflejadas opiniones de otros expertos como el profesor Pegueroles de la Universidad Politécnica de Cataluña que indica como actualmente usamos varios sistemas de pagos electrónicos, bien sea Visa o PayPal, los cuales tienen nombre y dejan un rastro. Sin embargo, en el caso del Bitcoin ocurre como con el dinero en metálico, es decir, cambia de manos sin dejar rastro. A partir de ahí, es inevitable que asalte la duda de si es una forma fácil de mover dinero negro. En el mismo artículo de Galtés encontramos más opiniones de otros autores como el Nobel Paul Krugman, que añaden como ventaja de Bitcoin que no se deprecia, pues el número de monedas está limitado desde su creación.

Una de las principales críticas es el uso de Bitcoin como un instrumento de especulación y generar burbujas. En el blog de Xavier Sala i Martín[16], podemos ver explicado un ejemplo de cómo se emplea el Bitcoin con usos especulativos. Por otro lado, explica que la principal función de Bitcoin es ser un medio de intercambio, aunque haya otras personas que lo usan como medio de inversión. El artículo del blog continua con un comentario respecto al precio de la moneda, el cual no se ve solo afectado por la oferta, sino que también puede variar en función de la demanda. En dicha explicación se apoya para argumentar que los compradores de Bitcoin son especuladores.

Gus Farrow, analista de divisas nos explica en la página FXstreet.com como no se puede entender el Bitcoin como un competidor en el mercado de divisas. Para este analista los que accedieron al comienzo de Bitcoin son los que han hecho negocio, sin embargo, para el público general está más alejado, pues no hay confianza. No obstante, con lo comentado anteriormente no se quiere enuncia que no haya futuro para el Bitcoin. Explicado de una forma más simple seria: si la población cree en su valor, si habrá un futuro. Las oportunidades y riesgos deben estar bien definidos, por lo que se precisa un tiempo.

Se puede concluir este apartado indicando, que, en la actualidad, Bitcoin es considerada la pionera de las múltiples criptomonedas existentes, que se puede utilizar como medio de intercambio para la adquisición de bienes y servicios en aquellos canales que sea aceptada y que es un instrumento de inversión. Su abreviatura es BTC.

[16] http://www.salaimartin.com/randomthoughts/item/589-la-burbuja-del-Bitcoin.html Consultado 03/04/2019

3.1.2 Origen del Bitcoin

Una vez hemos definido que es el Bitcoin pasaremos a explicar su origen, es decir, donde surge la idea y quien o quienes la ejecutan.

El propósito era crear una moneda descentralizada y con costes de intercambio bajos entre los usuarios[17].

La primera vez que apareció el término Bitcoin fue en un artículo llamado “Bitcoin: A Peer-to-Peer Electronic Cash System” firmado por Satoshi Nakamoto (2008). En el artículo se presenta a Bitcoin como el resultado de la combinación de varias tecnologías con la finalidad de obtener un método de pago descentralizado y vía electrónica.

El nacimiento de Bitcoin coincide con los años de mayor crudeza de la crisis financiera internacional y con las intervenciones de las autoridades monetarias, Reserva Federal, Banco de Inglaterra, Banco Central Europeo…con sus programas de liquidez y los consiguientes efectos sobre los tipos de cambios de las monedas. La situación de dificultad en el sistema financiero genera además una gran desconfianza en el mismo. Este entorno justifica, en parte, el momento en el que aflora una divisa virtual descentralizada.

El creador o creadores de Bitcoin son un programador o conjunto de programadores bajo el seudónimo de Satoshi Nakamoto, cuya identidad o identidades no se han descubierto.

Bitcoin es, por tanto, la primera moneda criptográfica emitida. Aunque hemos de señalar que la idea aparece con anterioridad en un artículo de Wei Dai en 1998[18]. La idea de emplear la criptografía se encontraba presente en una lista de correo electrónico que envió Wei Dai, que planteaba la idea de usar la criptográfia para crear un sistema electrónico para el intercambio de bienes y servicios al margen del control gubernamental (Plassaras, 2013). Esta moneda b-money no se llegó a emitir.

Satoshi Nakamoto público en 2008 el protocolo de Bitcoin. En 2009 nace el primer software conocido como Bitcoin Core quien fue el origen de la red Bitcoin y diversas monedas digitales. Satoshi Nakamoto dejo el proyecto en 2010.

En la figura 3.1 se recogen los hechos más importantes con relación a bitcoin en sus primeros cinco años de existencia.

[17] La idea de una moneda privada exenta de la influencia de los intereses de la política monetaria, que subyace en el origen de esta criptomoneda, fue introducida por Hayek (1976)

[18] http://weidai.com/bmoney.txt consultado el 22/05/2019

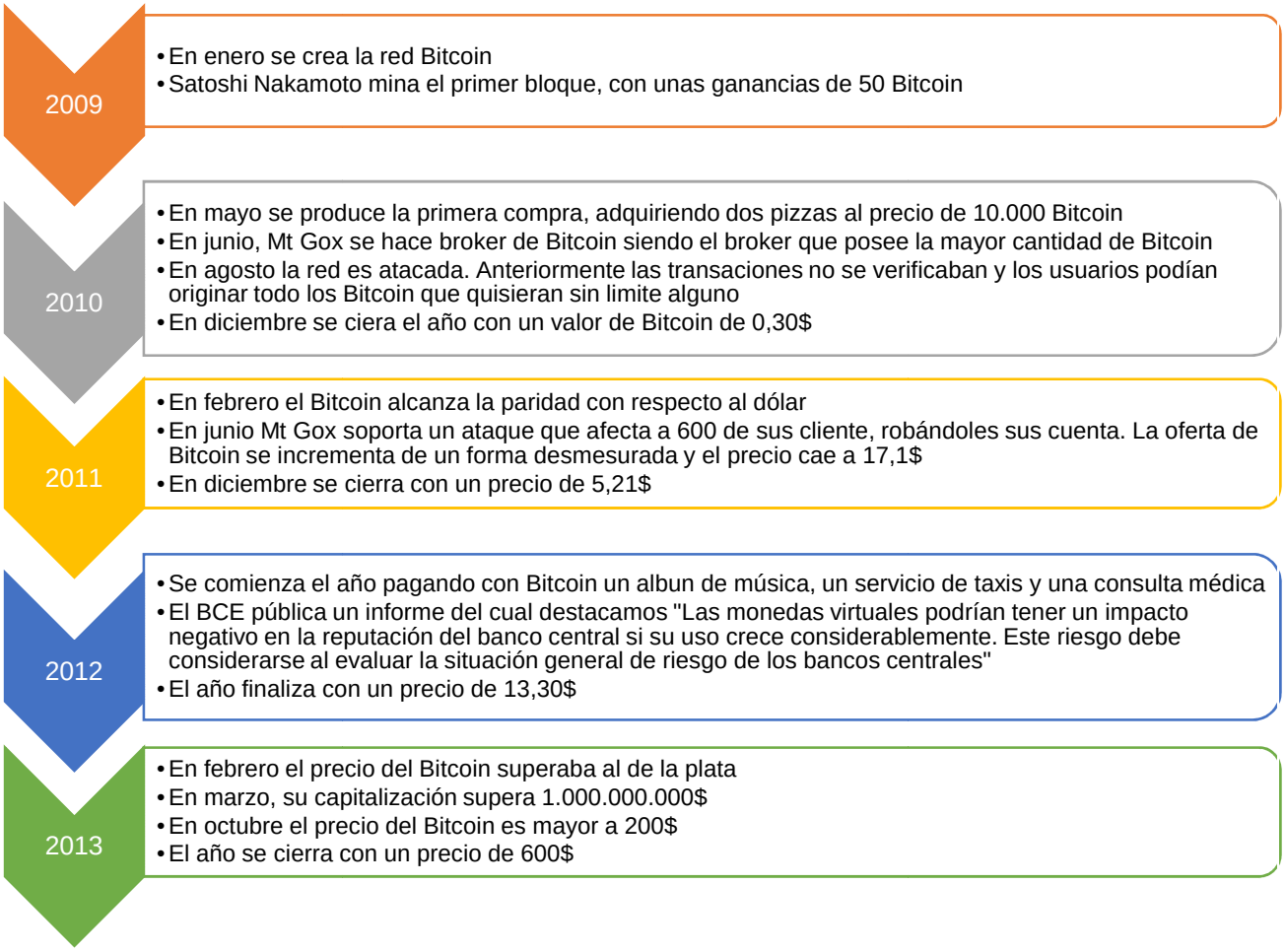


Figura 3.1. Línea cronológica del Bitcoin

Fuente Elaboración propia a partir de gurusblog.com[19]

3.2 ASPECTOS BÁSICO

3.2.1 Características del Bitcoin

En la figura 3.2 se recogen de forma resumida cuales son las principales características de Bitcoin

[19] https://www.gurusblog.com/archives/historia-Bitcoin/14/12/2013/4/ Consultado el día 26/05/2019

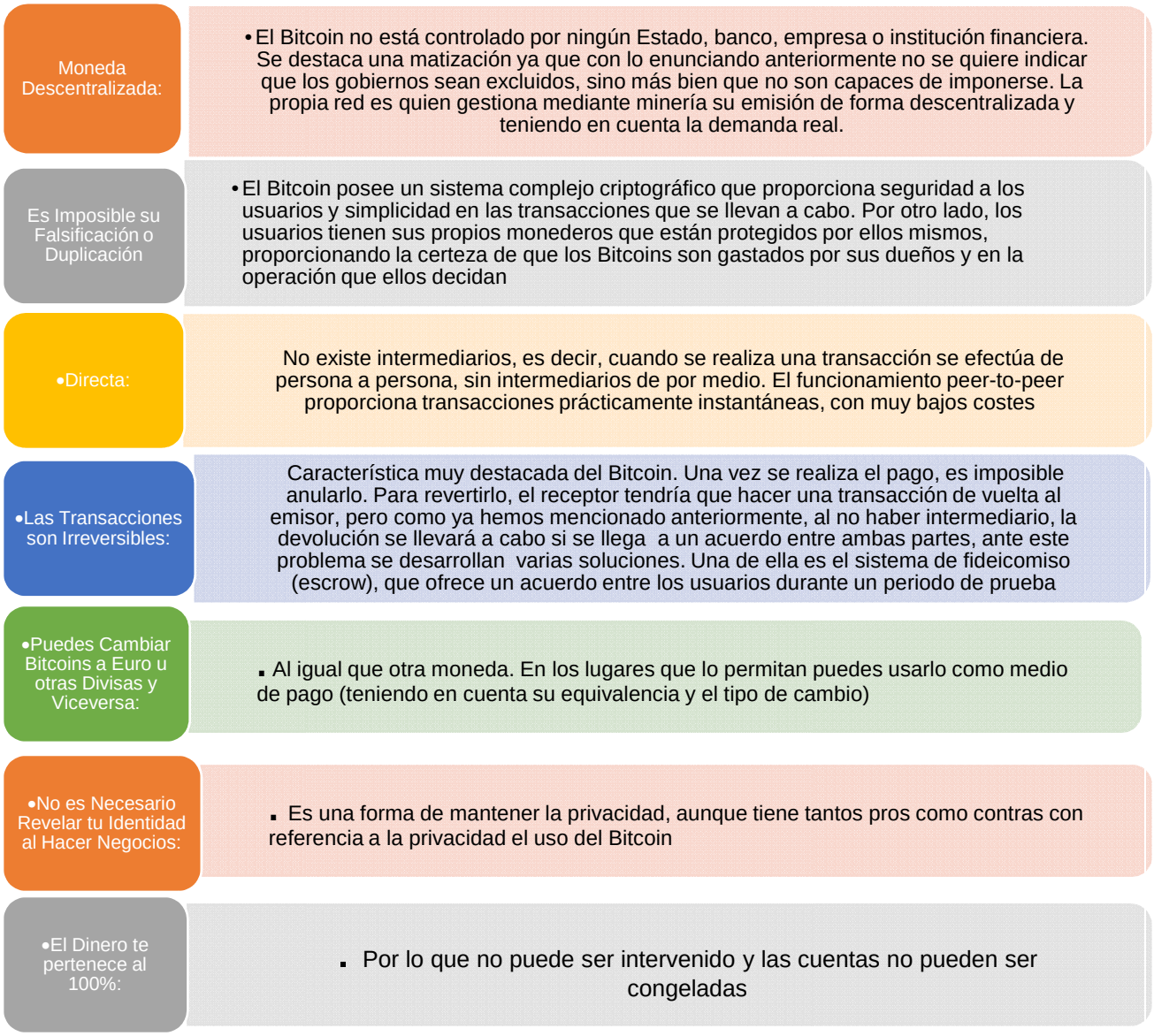


Figura 3.2 Características del Bitcoin

Fuente: Elaboración propia

Una vez hemos definido que es el Bitcoin vamos a pasar a explicar cómo funciona, así como conseguirlos.

En primer lugar, nos referiremos al funcionamiento de Bitcoin cuando lo que se pretende es obtener unidades de la criptomoneda para operar con ellas a través de la red.

Si entramos en la página de Bitcoin (The Bitcoin Foundation) podemos ver una explicación de cómo es su funcionamiento, aunque en primer lugar nos plantea una pregunta “¿Qué nos debemos plantear cuando somos usuarios nuevos?".

Podemos establecer un símil entre el funcionamiento del Bitcoin y el del correo electrónico. El correo electrónico lo usamos para mandar y recibir información, para que este intercambio de información sea posible nos servimos de direcciones de correo electrónico, es decir los correo son mandados o recibidos a una dirección concreta.

Otra pregunta que nos puede surgir es que, si es necesario entender el Bitcoin para poder operar con él, a lo cual responderemos de una forma negativa, es decir, no es

necesario entender a la perfección los conocimientos teóricos para usarlo, permitiendo su manejo a cualquier persona que posea unas leves nociones sobre el uso de Internet.

El primer paso que hay que dar para poder operar con Bitcoin es crearse una cuenta y un monedero, el cual se explicara en el siguiente apartado.

Una vez hemos visto lo que es un monedero y cuales son algunos de los tipos que hay se hace referencia a la generación de unidades de la criptomoneda.

3.2.2 Monedero

Un monedero (o como se conoce en inglés wallet Bitcoin) es un software que cumple la misma función que una cartera física, es decir, almacenar el dinero y en este caso, las monedas virtuales. Otras de las funciones que cumple esta cartera es la de permitir al usuario o dueño de esa cartera el poder enviar y recibir criptomonedas. Existen monederos que solo aceptan un tipo de moneda y otros que acepta varios tipos de criptomonedas. Estos monederos ofrecen seguridad a los usuarios con una serie de claves privadas, públicas y un sistema de criptografía.

Para comenzar a operar con Bitcoin hay que registrarse desde un ordenador o móvil. Una vez registrado y, a través de la aplicación informática, se genera un monedero donde se almacenan los Bitcoin. Este monedero esta enlazado con la dirección y ofrece la opción de generar más direcciones.

La dirección general, es la que se usa para enlazar las transacciones y tiene como destino el monedero. Bitcoin propone que las direcciones solo se usen una vez, así tenemos un anonimato mayor en cada transacción.

A continuación, en la figura 3.2 aparece la imagen que nos mostraría en la pantalla un monedero.

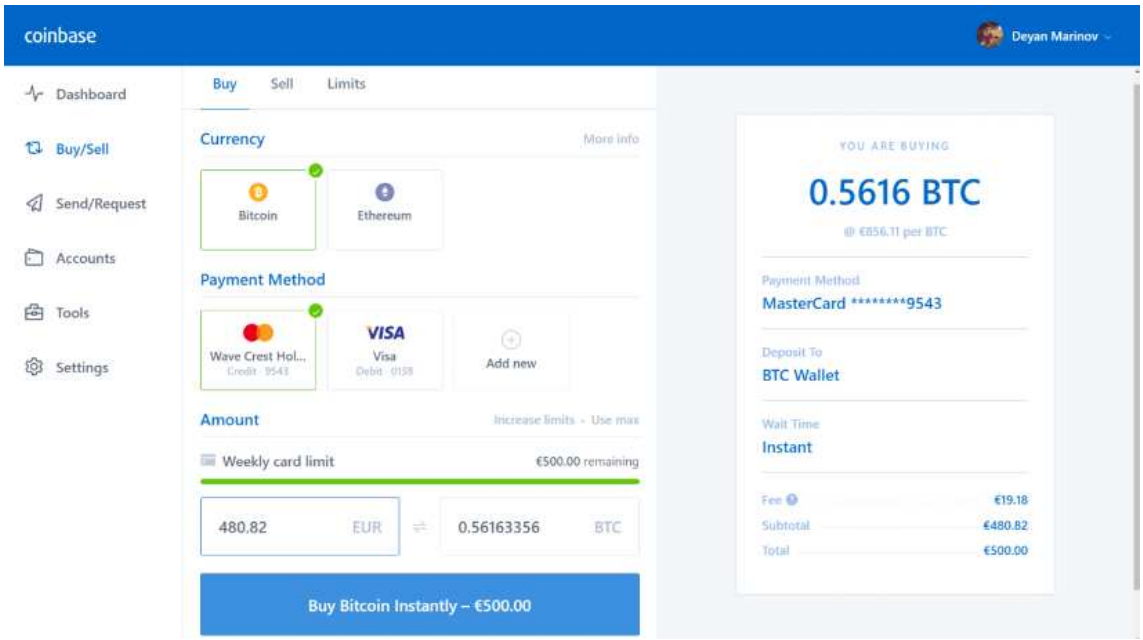


Figura 3.3 Monedero Coinbase

Fuente: Xataka.

En la figura 3.3 se observa como el usuario esté comprando Bitcoin. En la columna izquierda se encuentra las diferentes opciones que ofrece la cartera como por ejemplo

comprar o vender criptomoneda, mandar o recibirlas. También incluye una función donde se muestra una serie de gráficas y análisis.

En la figura 3.3 también encontramos las cuentas, que muestra los monederos que el usuario tiene a su disposición con sus saldos de la divisa que corresponda (ya sean euros, dólares, Bitcoin o Ethereum).

Este monedero ofrece una opción que se conoce como “herramienta” que permite ver las direcciones de pago para poder verificarlas e incluir las nuevas. Por último, también te muestra el historial de las operaciones realizadas.

En la parte central de la imagen, se muestra como el usuario ha marcado la opción comprar, a continuación, tiene la posibilidad de comprar o Bitcoin o Ethereum. Una vez decidido se pasa a seleccionar el método de pago como en una página normal de compra de internet.

Seguidamente aparece un límite de la tarjeta semanal de 500€. Y por último la conversión de, en este caso, euro a Bitcoin.

Este usuario ha invertido 480,82€ y como el precio ese día era de 856,1098€ obtiene 0,5163 BTC.

Existe una gran cantidad de monederos, cuyo uso depende entre otros aspectos del soporte que se utilice para operar. Los podemos clasificar según tenga el soporte ordenador, tablet o móvil. En la tabla 3.1 podemos encontrar algunos de ellos y algunas de sus características a modo de ilustración.

Soporte	Nombre	Características
Ordenador	**Bitcoin Core**	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa × Entorno vulnerable ✓ Privacidad mejorada ✓ Control total sobre las tarifas
	Bitcoin Knots	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa × Entorno vulnerable ✓ Privacidad mejorada ✓ Control total sobre las tarifas
	Wasabi	✓ Control sobre su dinero ✓ Transparencia completa × Validación centralizada × Entorno vulnerable ✓ Privacidad mejorada ✓ Sugiere la tarifa según transacción

	Electrum	✓ Control sobre su dinero ✓ Validación completa ✓ Buena transparencia ✓ Autenticación de dos pasos ✓ Privacidad mejorada ✓ Control total sobre las tarifas
Tablet	**Ledger Nano S**	✓ Control sobre su dinero ✓ Validación completa ✓ Basic transparency ✓ Autenticación de dos pasos ✓ Privacidad mejorada ✓ Variable libre de control
	Trezor	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa ✓ Entorno muy seguro ✓ Privacidad variable ✓ Variable libre de control
	BitBox	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa ✓ Entorno muy seguro ✓ Privacidad variable ✓ Variable libre de control
	KeepKey	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa ✓ Entorno muy seguro ✓ Privacidad variable ✓ Variable libre de control
	BitGo	✓ Control compartido sobre tu dinero × Validación centralizada × Aplicación remota ✓ Privacidad básica ✓ Autenticación de dos pasos

		✓ Sugiere la tarifa según transacción
	BTC.com	✓ Control compartido sobre tu dinero × Validación centralizada × Aplicación remota ✓ Privacidad básica ✓ Autenticación de dos pasos ✓ Sugiere la tarifa según transacción
	Coin.Space	✓ Control sobre su dinero × Validación centralizada × Aplicación remota × Entorno vulnerable ✓ Privacidad básica ✓ Sugiere la tarifa según transacción
Móvil	**Bitcoin Wallet**	✓ Control sobre su dinero ✓ Validación completa ✓ Transparencia completa ✓ Entorno muy seguro ✓ Privacidad variable ✓ Control total sobre las tarifas
	Bither	✓ Control sobre su dinero × Privacidad débil ✓ Validación simplificada ✓ Buena transparencia ✓ Entorno seguro
	BitPay	✓ Control sobre su dinero × Validación centralizada ✓ Privacidad básica ✓ Buena transparencia ✓ Entorno seguro ✓ Tarifas dinámicas con anulación

Tabla 3.1 Tipos de monederos[20]

Fuente: Elaboración propia a través de Bitcoin.org[21]

[20] Con un v se representa los aspectos positivos del monedero y con una × los aspectos negativos

[21] https://bitcoin.org/es/elige-tu-monedero consultado 16/05/2019

3.2.3 Transacciones

Supongamos dos usuarios, usuario A y usuario B. Imaginemos que el usuario A le quiere transferir al usuario B una cantidad determinada de Bitcoins, por lo que el usuario A debe renunciar a su posesión incorporando la clave pública de B y firmando la transferencia con su clave privada (la del usuario A), para poder verificar la propiedad de los Bitcoins. La información que hemos descrito previamente se trasmite a través de la red P2P. A continuación, los nodos verifican que el usuario A dispone de dicha cantidad de Bitcoin en su billetera y que además la transferencia está bien firmada. Si está todo correcto, la operación se incluye en la Cadena de Bloques, es decir, se incorpora a una base de datos que se replica en tiempo real en cada nodo. Por consiguiente, tendremos millones de copias de base de datos distribuidas por los equipos a lo largo del mundo.

La cadena de bloques está formada por registro de orden público, gracias a ello podemos ver qué operación han sido registrada, incluida las de tiempo real. El sistema de red Bitcoin tiene una transparencia sin precedentes en comparación con el sistema bancario.

Contamos con varias aplicaciones y sitios web que favorecen la actividad de interrogar a la Cadena de Bloque, un ejemplo sería blockchain.info.[22]

Todas las transacciones que se efectúan mediante la red no son aceptadas. Hay veces que se cometen errores, ya sea siendo consciente o de forma inconsciente, un ejemplo de ellos es el llamado “doble gasto”. Dicho trabajo se les atribuye a los nodos generadores, más conocido como los mineros.

Los equipos mineros adjuntan en un archivo el número total de operaciones que hay que verificar, anexo al último bloque aceptado de la cadena de bloques del que hay conocimiento. A partir de ese momento se da por iniciada una competición entre los mineros para ver quién es el más rápido en obtener el código aleatorio que identifica ese bloque (Hash) aplicando el método de prueba y error. El primer minero que se hace con la respuesta lo transmite a la red Bitcoin, los mineros restantes lo verifican y finalmente es añadido a la cadena de bloque.

Minar un nuevo bloque supone un gran esfuerzo computacional, el cual obtiene como beneficio un nuevo lote de Bitcoin que se le otorga al minero más rápido en conseguir el Hash. En los primeros años realizar esta tarea era muy rentable por la recompensa que se obtenía en Bitcoin, pero que en la actualidad esa recompensa ha disminuido como comentaremos posteriormente.

Los mineros son cruciales para el soporte del sistema, pues en ellos recae la labor de verificar las transacciones e ir actualizando la base de datos distribuida para que no se quede obsoleta.

3.2.4 Generación

Mediante el desencriptado de algoritmos matemáticos podemos generar Bitcoin, los cuales están basado en el modelo SHA-256 (es un sistema Secure Hash Algorithm[23], el cual posee una extensión de 256 bits), desarrollado por los clientes que se encargan de encriptar dentro de Bitcoin.

[22] Se trata de un servicio que permite a los usuarios saber que ocurre en la red Bitcoin. Ofrece gráficas y análisis. https://www.blockchain.com/es/ consultado 21/03/2019

[23] Sobre los algoritmos Hash puede consultarse a Escalona e Inclán (2012)

La generación de Bitcoin corresponde a los denominados mineros. Es una forma de comparar la adquisición de nuevas criptomonedas con la actividad de obtener oro u otros metales preciosos de la mina.

Cada diez minutos, la red genera y pone a disposición un nuevo paquete de Bitcoin, que se distribuyen como un premio a los mineros. La cantidad de Bitcoin que va en los lotes ha ido variando con el pasar del tiempo, en la actualidad están formados por 25 Bitcoin. El sistema está programado para producir una cantidad limitada de Bitcoins, provocando que el nivel de dificultad para acceder a ellos varia con el transcurrir del tiempo. Está previsto un límite máximo de emisión de Bitcoin, la cifra es de 20.999.999 Bitcoins y se alcanzará en 2140. La creación de Bitcoin se realiza mediante una progresión geométrica por lo que en 2019 se ha llegado a alcanzar los 16,8 millones. Si lo pasamos a porcentaje representa el 80%, quedando por minar unos 2,4 millones que están previsto que se minen hasta el 7 de mayo de 2140.

Para poder minar es necesario equipos informáticos que cada vez sean más ponentes. El hallar el Hash de los bloques nuevos proporciona una gran rentabilidad, haciendo que el número de usuarios interesado crezca en parámetros vertiginosos, por otro lado, el nivel de competencia es bastante elevado. En los inicios del proyecto, se usaba un ordenador de sobremesa. Actualmente se ha producido una revolución con respecto al desarrollo de equipos diseñados específicamente para la minería Bitcoin, los cuales cuentan con 500 Gigas Hash/s, es decir, ordenadores capaces de ejecutar 500.000.000.000 comprobaciones del Hash del bloque en un segundo, por una cuantía que supera los 22.000$. Sin embargo, este tipo de ordenador tan potente no es capaz de asegurar en varios meses la obtención de un solo lote de Bitcoin. Los mineros a modo de solución han optado por unirse a grupos llamados “pools” para incrementar la potencia de cálculos y no hacer comprobaciones dobles. Estos pools reparten el beneficio de una forma proporcional a la potencia del cálculo que ha ofrecido cada uno de los integrantes del grupo.

Existe otra forma de premiar la tarea que realizan los mineros en el sostenimiento de la red. Los mineros son recompensados con el ingreso de las comisiones que el usuario debe pagar al realizar una transacción. De tal modo, el minero que acepta la operación en su bloque y se dispone a verificar, será recompensado con unos cuantos céntimos de Bitcoin. Las transferencias que incluyen una recompensa son tratadas con mayor rapidez.

3.3 OTROS CONCEPTOS DE BITCOIN

3.3.1 Definición de los Blockchain

Nació como “la mano derecha” de Bitcoin, no obstante, puedes llegar a ser actualmente una de las tecnologías más vulnerables. La finalidad del blockchain es el desarrollo de una tecnología que acepte el intercambio peer-to-peer, dicho con otras palabras, gracias al blockchain se puede ejecutar transferencias de una forma directa en la red sin tener que existir de por medio un intermediario.

Según nos muestra Mac Andreessen (2014), quien creo Netscape y forma parte en uno de los fondos de Capital Riesgo más significativo de Silicon Valley “Una cadena de bloques es esencialmente sólo un registro, un libro mayor de acontecimientos digitales que está “distribuido” o es compartido entre muchas partes diferentes”.

El Blockchain está formado por dos agentes, de un lado se encuentra el libro contable distribuido (distributed ledger) y de otro lado tenemos el contrato inteligente (smart contract). La información integrada de la criptomoneda que se modifica o bien se intercambia se quedará guardada en el distributed ledger, de tal forma que todo

cambio o modificación que se realice será informado, evitando cualquier manipulación o pérdida de datos.

Denominamos bloques a las transacciones que se realizan, las cuales están codificadas y vinculadas a otros.

Como ya hemos comentado anteriormente, la información esta guardada en la red y en un gran número de ordenadores, siendo pública para todo el mundo. Gracias a ello podemos decir que es un proceso transparente y resistente a modificaciones. Para que se apruebe la información suministrada es necesaria que la comunidad que forma la red Bitcoin llegue a un acuerdo.

3.3.2 ¿Cómo funciona la cadena de bloques?

Blockchain posee un registro de todas las operaciones que se han llevado a cabo desde el comienzo del Bitcoin, en función de ella se fija el número de Bitcoin que acumulan los monederos.

A continuación, se va a explicar tres términos esenciales para entender el blockchain. En primer lugar, se encuentra el concepto “Hash”. Hash no es más que un algoritmo cuya función es reunir información de una longitud determinada, la cual una vez tratada se transforma en información con una longitud estandarizada, denominando al valor “Hash”.

El proceso Hash es usado en el mundo informático para poder operar con una gran cantidad de información y poder explorarla. Hash limita la información, es decir, para la misma información recibida solo hay una información alcanzada por lo que el valor Hash no cambiará

Bitcoin se sirve del proceso Hash para comprobar y registrar las transferencias, aunque en el sistema de Hash hay ciertas limitaciones, por ejemplo, la función Hash solo puede ser de una dirección por lo que, aunque tengamos el resultado no es posible saber el origen, proporcionando al Bitcoin un carácter pseudo-anónimo. Como ya hemos mencionado anteriormente, la información semejante no puede contener un valor diferente.

En segundo lugar, tenemos el término “Time-stamp” el cual se define como un examen para localizar un documento digital en un determinado momento. Sus usos son muchos y variados, los cuales abarcan desde certificar un contrato hasta confirmar una transacción que se ejecuta de forma electrónica. Bitcoin se sirve del término Time-stamp para incrementar la seguridad de las transacciones. Posteriormente comentaremos como en el momento de la comprobación se revisan las fechas de transacción.

En tercer y último lugar encontramos el concepto “proof-of-work”, consiste en un protocolo de confinaciones de las comunicaciones que el usuario lleva a cabo con el servidor. En primer lugar, el usuario se comunica con el servidor para obtener el servicio. A continuación, el servidor le formula una cuestión que el usuario debe solucionar. Para finalizar, el servidor comprueba que la cuestión planteada se ha solucionado de forma correcta y permite el acceso al servidor. Un aspecto positivo a destacar es la dificultad leve que posee, capacidad que Bitcoin emplea para normalizar la fabricación de dinero a lo largo del tiempo.

Bitcoin emplea las ideas comentadas anteriormente para obtener una base de datos de carácter pública y segura, dando lugar al blockchain. El blockchain se forma por una serie de bloques que se encuentra unidos entre ellos. Las nuevas operaciones que se producen se almacenan en bloques, que se van añadiendo al último bloque. De la seguridad de los bloques se encarga el protocolo proof-of-work. Si queremos realizar una modificación hay que aprobar un procesamiento similar al que había, en

otras palabras, crear una “cadena alternativa”. Debido a que el número de procesamiento que se requiere es muy costoso y de una dificulta elevada, es materialmente imposible realizar una modificación.

Llamamos “Bloque Padre” al bloque precursor. Al primer bloque se le asigna el nombre de “Bloque Génesis”, cuyo padre fue Nakamoto, seudónimo que se la atribuye al creador del Bitcoin. El bloque concluyente se denomina “Bloque Líder”. Con lo redactado anteriormente no se pretende dar a entender que la cadena sea enteramente lineal, pues en muchas ocasiones la cadena de bloque comete errores dando lugar a varios caminos a partir del “Bloque Líder”. El sistema está configurado para que uno de los dos caminos sea condenado dando lugar a los “Bloques Huérfanos”.

A continuación, en la figura 3.2 se muestra un ejemplo de una cadena, donde en primer lugar se encuentra al bloque génesis. Esta cadena se fragmenta en dos partes, una de ella es condenada a ser eliminada de esa cadena obteniendo como resultado un bloque huérfano. La parte restante da lugar al bloque líder.

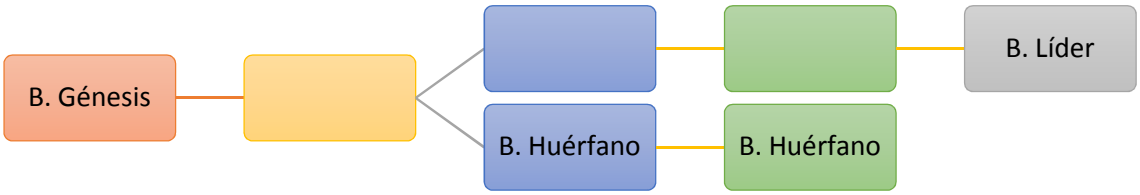


Figura 3.4 Ejemplo de una cadena de Bloque

Fuente: Elaboración propia

La situación reflejada en la figura 3.4 se llama un “tenedor” en la cadena. Se produce cuando hay dos mineros que han llegado al mismo bloque al mismo tiempo, es decir, ambos encontraron la solución al enigma Hash, aunque solo uno de los bloques obtenidos puede formar parte de la cadena. Este fallo provoca que haya dos caminos durante un número de bloques hasta que uno sea condenado a desaparecer de esa cadena dejando solo un camino. Debemos resaltar que con lo explicado anteriormente no queremos decir que las transferencias que integren los bloques huérfanos sean abandonadas, pues el sistema las incluye de nuevo al espacio donde se encuentra las transferencias que están esperando a ser resueltas.

Capítulo 4. Fortalezas y debilidades de Bitcoin

En el anterior capitulo presentamos un estudio acerca del Bitcoin, pasando por sus características, funcionamiento y tipos de monederos que existen. En el presente capitulo nos centraremos en el estudio de las ventajas y desventajas que existen acerca de esta criptomoneda. Por otro lado, también haremos mención a la seguridad que posee las criptomonedas.

4.1 VENTAJAS E INCONVENIENTES DEL BITCOIN

El Bitcoin no está sometido a ninguna organización. Como se ha ido explicando a lo largo de los distintos capitulo, el concepto de dinero electrónico descentralizado es algo relativamente nuevo y que no está instaurado como por ejemplo el dólar o euro, como consecuencia de ello la cima o auge del dinero electrónico es un acontecimiento que tiene que construirse e implantarse.

No obstante, a partir de 2013 conforme comenzaron a aumentar el número de operaciones con Bitcoin y la divisa aumento su cambio con respecto a otras monedas de curso legal comenzaron a publicarse distintos trabajos en los que se resaltaban las ventajas e inconvenientes que estas criptomonedas presenta. Trabajos de los bancos centrales de Inglaterra (Ali, et al., 2014), Banco Central Europeo (2012) entre otros destacan las principales desventajas de la misma.

En otros trabajos como en Navas (2015), Sarmiento y Garcés (2016), Rivas (2016) y Torres (2015) se muestra las ventajas e inconvenientes que las criptodivisas presentan.

En estos trabajos que citamos nos hemos basado para exponer las ventajas y limitaciones de Bitcoin que se recogen respectivamente en los dos siguientes apartados

4.1.1 Ventajas del Bitcoin

✓ Gracias a que el Bitcoins es libre y descentralizado podemos decir que Bitcoin es una moneda democrática y participativa. Con Bitcoin nació la primera red de pago que se mueve por los usuarios y no por las autoridades centrales, es decir, los usuarios tienen el control total de sus billeteras.

✓ Bitcoin fue pensado para Internet, gracias a ello brinda opciones puntuales a numerosos sistemas antiguos que son caros y pesados. Bitcoin es defensor y partidario del micro-pago, acercando a los usuarios la posibilidad del pago electrónico a mercados en los que anteriormente no se barajaba como una alternativa debido a los costes tan elevado que estos suponían.

✓ Bitcoin proporciona libertad y preserva los derechos de sus usuarios. Cuenta con un sistema que acepta que los clientes almacenen e intercambien valores de una forma segura a través de la red sin que puedan ser descubierto, falsificado o interceptada por una organización o bien por un individuo.

✓ Como ya hemos mencionado anteriormente, Bitcoin es una moneda global y neutra, es decir, el influjo político o economía nacional no puede incidir en ella. También tiene un carácter universal llegando hasta localizaciones donde la banca no ha llegado.

✓ Las transacciones que se realizan son públicas, por ellos podemos enunciar que indiferentemente del anonimato de los usuarios, Bitcoin es transparente.

✓ Bitcoin emplea las reglas criptográficas de una forma inteligente, pudiendo asegurar las transacciones. Las reglas criptográficas brindan una cantidad elevada de funcionalidades que proporcionan una seguridad incrementada. Es impensable el manipular el Bitcoin o su protocolo de seguridad.

✓ Con Bitcoin es posible ahorrar pues nos ofrece operaciones directa y libre de comisiones o cargos bancarios, esta característica es muy beneficiaria para los pagos internacionales.

✓ No podemos hablar de inflación de Bitcoin, pues el número de Bitcoin generados está estudiado con anterioridad a la cantidad máxima de 21 millones de Bitcoin. Esto provoca que no haya inflación por lo que podemos decir que "Bitcoin protege la inflación". Debemos indicar que los Bitcoin que se han perdido por los usuarios jamás serán reemplazados.

4.1.2 Limitaciones del Bitcoin

× El procedimiento de puesta en el mercado puede dar lugar a discusión. Los primeros usuarios que entraron a usar la red Bitcoin son los que mejor se han beneficiado con respecto a la generación de Bitcoin de una forma individual, aunque a día de hoy es muy difícil generarlo así.

× El comprar Bitcoins es algo "ridículo" aunque sea esta la mejor forma de obtenerlos. Explicando un poco lo enunciando anteriormente, el euro actualmente está vigente en la totalidad de las páginas de Internet, por lo que resultaría poco inteligente el obtener una moneda para gasta en internet si ya existe el euro.

× Bitcoin es muchas cosas, pero ante todo es volátil. La finalidad de los usuarios que adquiriente Bitcoin es, en la mayoría de los casos, el intercambio con dólares o euros sirviéndose de la especulación y no como forma de obtener bienes o servicio.

× Bitcoin es una oportunidad de oro para las mafias gracias al anonimato que proporciona al realizar las transacciones y al poco control y frontera que existen. Por ello es la forma de pago más recurrente en la Deep Web o en español Internet Oscuro.

× Si nos centramos en la poca formación de la población con respecto al Bitcoin, podemos decir que es una moneda inalcanzable. Una gran cantidad de población no están capacitado para depositar sus ahorros en cualquier tipo de las monedas virtuales que existen, pues hay monedas que si no se conocen bien pueden de un momento a otro fugarse.

× La cantidad de operaciones que Bitcoin permite es reducida, pues la red no está capacitada para manejar más de siete transferencias en un segundo, dicha cantidad es algo pobre para la tecnología que cuenta, la cual tienen fines más grandes, como por ejemplo ser un medio de pago.

4.2 SEGURIDAD ACERCA DEL BITCOIN

➢ En la página de Bitcoin encontramos un apartado que hace referencia a la seguridad Bitcoin, en la cual nos informa de que el protocolo y la criptografía cuentan con robusto historial en lo que a seguridad se refiere.

➢ En términos matemático es invencible y en ello argumenta su seguridad, de no ser así los distintos usuarios de todo el mundo no confiarían en la moneda. Si se sigue evolucionando e innovando en un futuro podríamos tener un algoritmo de cifrado y hash más factibles y seguros pues, se podría ir actualizando el sistema Bitcoin y sirviéndose de la tecnología más moderna ofreciendo una seguridad inmejorable.

- Los archivos de los monederos donde se almacena las claves privadas pueden ser borrados, perdidos o incluso robados de una forma accidental. Es muy semejante al dinero físico que se encuentra guardado de forma digital. No obstante, los usuarios cuentan con distintas prácticas de seguridad para resguardar el dinero, también cuenta con una serie de proveedores de servicios que brinda unos niveles altos de seguridad, así como una garantía que le protege de robo o pérdida.

- Aunque han pasado unos años desde que se creó el Bitcoin, sus reglas de protocolo, así como la criptografía empleada siguen actuando de una forma correcta, respaldando la idea que Bitcoin planteo en sus orígenes. Sin embargo, debemos matizar que a lo largo de la historia del Bitcoin se ha encontrado fallos de seguridad. Estos fallos se han subsanado cambiando el sofware.

- La seguridad de Bitcoin oscila en función de la rapidez en la que se encuentren los problemas y se solucionen, pues conforme se van encontrando problemas Bitcoin se ira enriqueciendo.

- Es muy común que haya tergiversaciones referentes a robos o a roturas de seguridad que se dan en transacciones o negocios. Estos acontecimientos son desfavorables para la imagen de Bitcoin, aunque ninguno de ellos llega hasta tal punto de hackear Bitcoin, del mismo modo que, por ejemplo, el robar un banco no quiere decir que el euro sea inseguro.

- En el último periodo se han diseñado nuevas pautas de seguridad, así encontramos la encriptación de cartera, monederos offine, monederos físicos o transacciones multi-firma entre otras.

- Es muy difícil el intentar cambiar las reglas de Bitcoin. Si hay un usuario que no esté cumplimiento con el protocolo de Bitcoin no podrá imponer el suyo al resto de usuarios. En las últimas actualizaciones no se puede incluir el doble gasto en la misma cadena de bloque, tampoco se puede desembolsar Bitcoin sin que exista una firma válida. Debido a ello es imposible el poder obtener un número desmesurado de Bitcoin de la nada, pagar con capital ajeno, manipular la red o actividades similares.

- No obstante, no se puede obviar el hecho de que un grupo voluminoso de mineros podrían bloquear o incluso restablecer operaciones que se han ejecutado recientemente. Por otro lado, un grupo grande de clientes podrían presionar para llevar a cabo cambios. El funcionamiento correcto de Bitcoin se debe a un consenso total de los usuarios que lo forman, este es el motivo por el que es tan difícil el intentar modificar las reglas del Bitcoin, ya que para que esto fuera posible, la gran mayoría tendrían que acoger la modificación y el resto minoritario aceptarlo sin más. No se puede olvidar que el fin de los usuarios de Bitcoin es ganar dinero, por ello resulta complicado que el usuario de Bitcoin acoja una modificación que afecta su dinero.

A continuación, enunciaremos algunos consejos que se recomienda a la hora de usar el Bitcoin:

- No dejar que nadie vea tu clave privada.

- Hacer uso de la función de cifrado que las aplicaciones de Bitcoin traen incorporadas.

- Tener una contraseña de más de diez caracteres, intercambiando números, letras mayúsculas y símbolos.

- Tener el ordenador libre de virus, así como de troyanos, sofware espías Keyloggers (que no son más que capturateclas).

- No usar carteras online en las cuales no se confían.

- Mantener el sotware actualizado y hacer uso de la doble autenticación.

- Realizar copias de seguridad.

- Utilizar direcciones multifirma.

CAPÍTULO 5: ANÁLISIS DE LA EVOLUCIÓN DE LAS PRINCIPALES MAGNITUDES DE BITCOIN

Continuando con el trabajo y una vez se ha analizado los beneficios y limitaciones que posee el Bitcoin, pasaremos a comentar su evolución. Nos apoyaremos en diversas gráficas y se aportarán algunos ejemplos para poder explicar, de una forma más sencilla, como ha ido evolucionando el Bitcoin.

5.1 LOS DATOS DE BITCOIN

A continuación, se va a realizar un análisis de la evolución que ha tenido algunos parámetros del Bitcoin desde el principio para así poder apreciar la dimensión del proyecto, y también el crecimiento del interés de los usuarios.

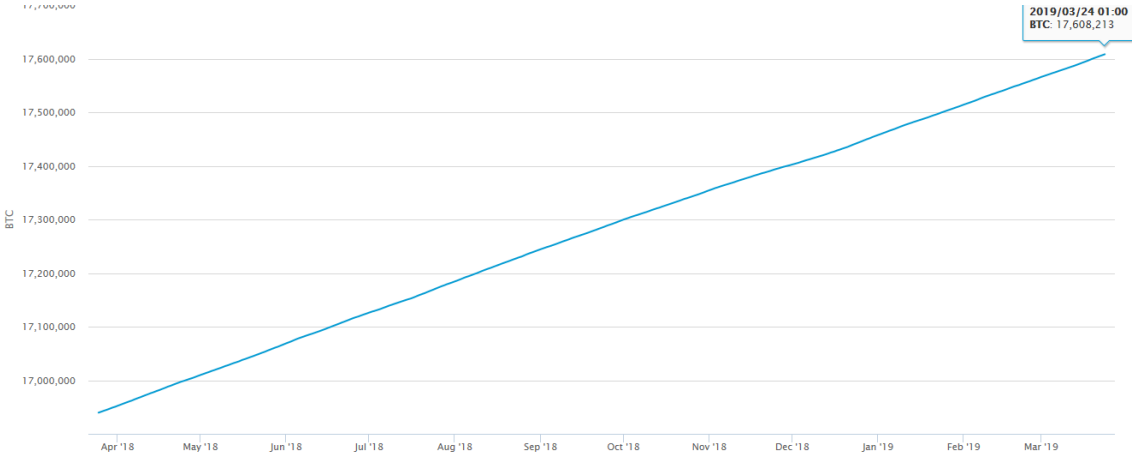


Figura 5.1 Número de Bitcoin emitidos

Fuente: Blockchain.info

A fecha de 24 de marzo de 2019 se habían emitido 17.608.213 Bitcoin. No obstante, esa cantidad de Bitcoin no está en circulación al 100%. El crecimiento que ha sufrido ha sido muy importante, aunque debemos matizar que parte de los Bitcoin que se han puesto en circulación, a la fecha en la que estamos se han perdido por errores. Las pérdidas de unidades de la moneda se deben fundamentalmente a que en sus orígenes la moneda tenía poco valor de cambio frente a otras monedas de curso legal y los mineros que inicialmente accedieron al proyecto no hicieron las copias de seguridad de las carteras electrónicas o perdieron sus claves.

El total de Bitcoin que se van a poner en circulación asciende a 21 millones. El crecimiento de la oferta de Bitcoin se debe a una serie geométrica, la cual tiene una razón constaste. En 2013 se había puesto en circulación la mitad de Bitcoin, la cifra rondaba los 11.288.300 Bitcoin, en 2019 se encuentra en circulación más de la 3/4 parte de la oferta dispuesta. Según nos muestra el blog Academy by Bit2me[24] se espera que conforme la cifra de Bitcoin se vaya acercando a los 21 millones, la economía de Bitcoin entre en deflación, es decir, el poder adquisitivo se verá incrementado hasta alcanzar la estabilidad.

[24] https://academy.bit2me.com/deflacion-en-Bitcoin/ consultado 21/05/2019

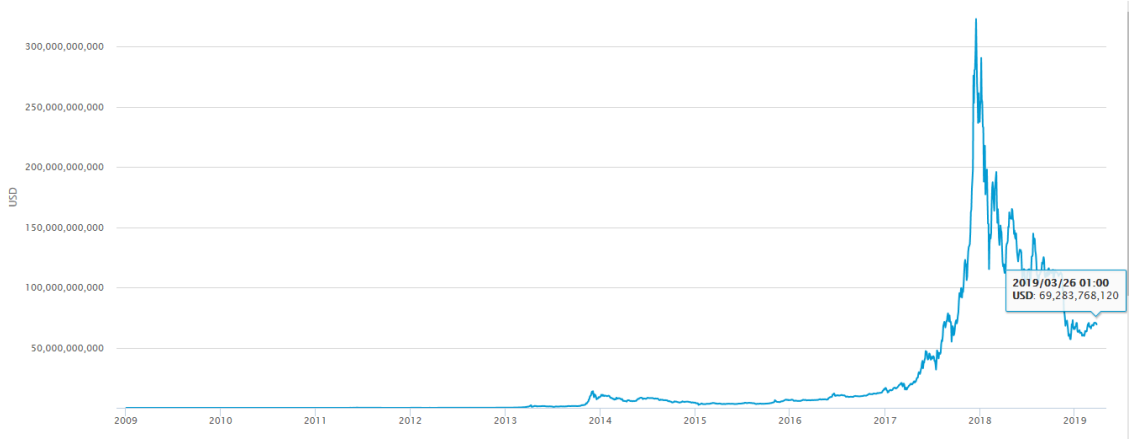


Figura 5.2 Capitalización del mercado

Fuente: Blockchain.info

En la gráfica 5.2 se muestra como ha ido evolucionando la capitalización del mercado. La capitalización se obtiene al multiplicar el número de Bitcoin por su precio. Como se observa, la capitalización del Bitcoin se mantuvo sin apenas cambios desde 2009 hasta 2013. En 2014 tuvo un pequeño incremento alcanzando el pico más alto el día 29/11/2014 con 13.065.737.063 USD. La cotización vuelve a caer situándose en 2015 en 4.278.907.103 USD y manteniendo esta cotización con pequeños movimientos hasta 2017. Desde ese momento la cotización frente al dólar fue al alza llegando a alcanzar su pico más alto en 2018 con 323.071.829.482 USD. En la gráfica se puede apreciar la alta volatilidad del valor del Bitcoin en el periodo 2017-19.

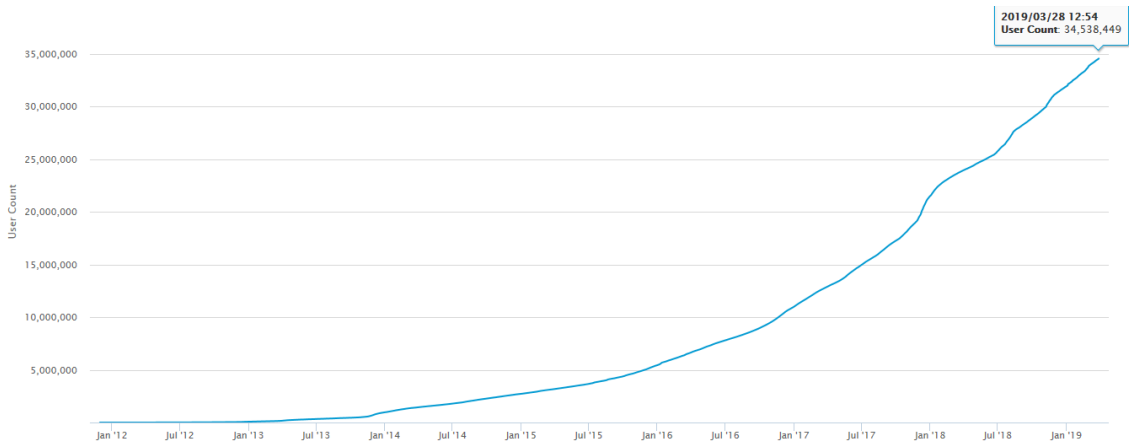


Figura 5.3 El número total de Blockchain Wallet creadas

Fuente: Blockchain.info

En la figura 5.3 se aprecia como la cantidad de usuarios que adquiere la aplicación conocida como Mi Monedero ha experimentado una evolución creciente desde que se creó, posicionándose actualmente en 34.538.449 usuarios. Mi Monedero es una cuenta Bitcoin que está siempre en línea. Nos ofrece la posibilidad de poder ejecutar pagos en cualquier lugar del mundo de forma anónima y sin ningún gasto. Gracias a esta aplicación se puede pagar con Bitcoin de forma segura y fácil y podemos utilizar para ello un ordenador o un teléfono móvil.

En la figura 5.4 se recogen el número de transacciones que se llegan a realizar en un día a través de la aplicación Mi Monedero. Observamos que en los primeros años en los que la moneda se pone en circulación y hasta prácticamente mitad de 2012 el número de transacciones con la moneda fue muy escaso. Sin embargo, a partir de ese

momento ha seguido una tendencia creciente hasta 2018. El mayor número de transacciones diarias se produce el 17 de diciembre de 2017, un total de 391.910[25], que como posteriormente recogemos coincide con el día en que Bitcoin alcanza su máxima cotización. Entre esa fecha y abril de 2018 se produce una caída en el número de transacciones diarias que se reduce a más de la mitad, pero a partir de entonces comienza de nuevo a crecer. El último dato consultado que corresponde a marzo de este año situaba el número de transacciones diarias por encima de las 383.000

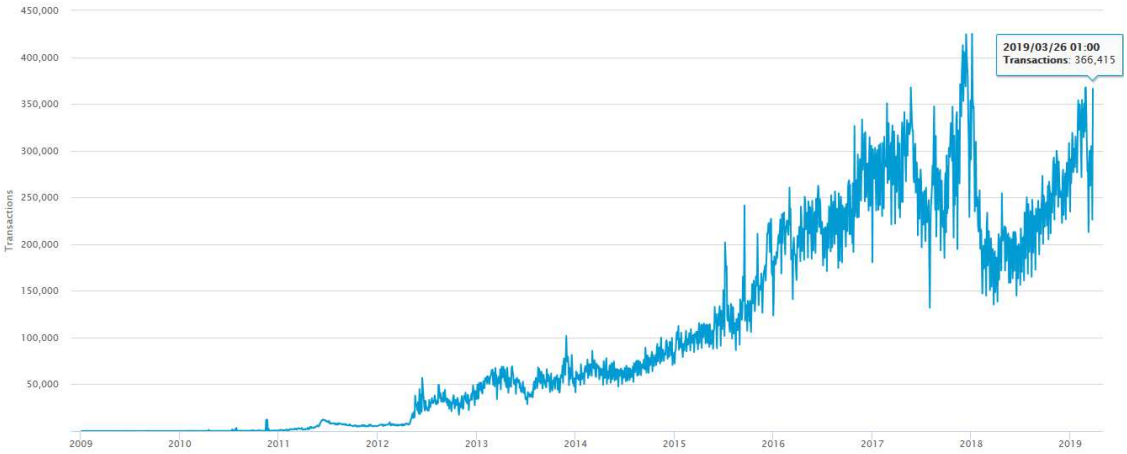


Figura 5.4 Número de transacciones por día con Bitcoin

Fuente: blockchain.info

Para completar el análisis de las cifras más relevantes de Bitcoin, en la figura 5.5 recogemos la evolución del cambio frente al dólar USA desde abril de 2014 hasta marzo de 2019. La oferta y la demanda son las que dictaminan el precio del Bitcoin frente a las denominadas monedas de curso legal.

Figura 5.5 Cotización de Bitcoin / Dólar Estadounidense

[25] El dato se ofrece en Blockchain Luxemburgo S.A. En https://www.blockchain.com/es/charts/n-transactions?timespan=all (consultado el 26 de abril de 2019).

Fuente: Trading View

La figura muestra cómo la cotización pasa de estar por encima de 900$ en 2014 a ni siquiera alcanzar los 277$ un año más tarde, el descenso continuo hasta llegar a los 245$ en 2015.

Lo descrito anteriormente no es más que un simple ejemplo de las distintas fluctuaciones que ha sufrido el Bitcoin desde sus orígenes. Uno de los más acentuados fue el paso de no tener valor alguno a presentarse con un valor de cotización de 19.891$ el 17 de diciembre de 2017.

Las gráficas que recogemos en este apartado nos muestran, por un lado, que se trata de una tecnología en crecimiento de uso desde su creación, como muestra el número creciente de monederos y monedas. Sin embargo, otros datos como son la cotización frente a otras monedas o la oscilación en las transacciones nos informan de una gran volatilidad.

5.1.1 Evolución del Bitcoin

En la página Investing.com[26] se recogen datos de cotización diaria del bitcoin frente al dólar desde 2 de febrero de **2012** hasta la actualidad. Concretamente, en esa primera fecha que referimos, la cotización fue de 6,10 dólares por bitcoin. Ese año cotizo entre el mínimo de 4,22 dólares y un máximo de 13,70, siendo el promedio de 8,50 dólares por bitcoin y la variación entre el precio máximo y mínimo del 122,20%.

En **2013** la cotización oscilo entre los 13,28 dólares por Bitcoin a comienzos del año y el máximo de 1.200 dólares por bitcoin que se alcanzó el 7 de diciembre de ese año. El precio promedio en ese año fue de 187,71$ por bitcoin y la variación de precio en el año superior al 5286%.

En **2014** se registraron caídas de las cotizaciones con respecto a las cifras alcanzadas a finales de 2013. Estas caídas fueron la consecuencia de que el gobierno chino suprimiera el Bitcoin, los bancos fueron forzados a clausurar las cuentas de las distintas casas de cambio que trabajaran con Bitcoin. La cotización máxima de ese año fue de 850$ y la promedio de 523,8$.

En **2015** se alcanza un máximo de 503,4$ por Bitcoin el 4 de noviembre y una cotización mínima de 164,9 en enero. El promedio de ese año fue de 278,8 dólares Bitcoin, lo que representa el 53,22% del precio promedio del año anterior.

En el año **2016**, el Bitcoin se inicia con una cotización de 434$, y cierra con una cotización de 966,6$. La cotización promedio de ese año fue 556,7 $.

El año **2017**, fue el de las fuertes subidas en la cotización. Comenzó por debajo de los 1.000 dólares y cerró en 13.800 dólares. Ese año llegó a alcanzar una cotización máxima 19.891$ el 17 de diciembre. Este año se produjo sucesos políticos significativos, como es el Brexit, la llegada de Trump a la presidencia de los Estados Unidos, la crisis de China, la política monetaria de India. En agosto de este mismo año nace el Bitcoin Cash

El año **2018** abre con los precios altos de 2017, la cotización máxima de ese año es 17.252 dólares el 6 de enero. La cotización experimenta en ese año sucesivas caídas, la mínima de 3.216,1 se produce en diciembre de ese año. La cotización promedio de este año fue de 7.550,4 dólares por Bitcoin.

[26] https://es.investing.com/crypto/bitcoin/btc-usd-historical-data

En lo que llevamos del presente año, la cotización de la moneda ha ido en ascenso. La apertura fue de 3.963 $ por bitcoin, la cotización máxima hasta el momento ha sido de 8.307,7 el 16 de mayo.

5.2 COTIZACIÓN BITCOIN, DÓLAR, EURO

A continuación, vamos a proceder a realizar un análisis de las tres monedas mencionada para saber si existe arbitraje entre ellas. Para realizar este análisis se utilizarán los tipos de cambio bitcoin por dólar USA (USD/BTC), Bitcoin por euro (EUR/BTC) y Euros por Dólar (USD/EURO) obtenidos de la paguina investing.com[27]

Para realizar dicho análisis nos hemos servidos de la hoja de cálculo Excel y los datos los hemos tomado para el periodo comprendido entre 05/11/2018 y 05/04/2019, de la página web mencionada en el párrafo anterior.

A partir de los datos se calcula el precio cruzado USD/EURO de la siguiente forma

$$\frac{USD/BTC}{EUR/BTC}$$

Este dato es necesario para poder contrastar si el precio era similar al del mercado o no, pues “en teoría”, debe ser el mismo. Si por el contrario no coincide se plantea la opción de que haya un arbitraje. En la figura 5.6 se representa ambos precios. Como se observa en la figura, ambos precios difieren, aunque están más próximo a comienzos y final del periodo.

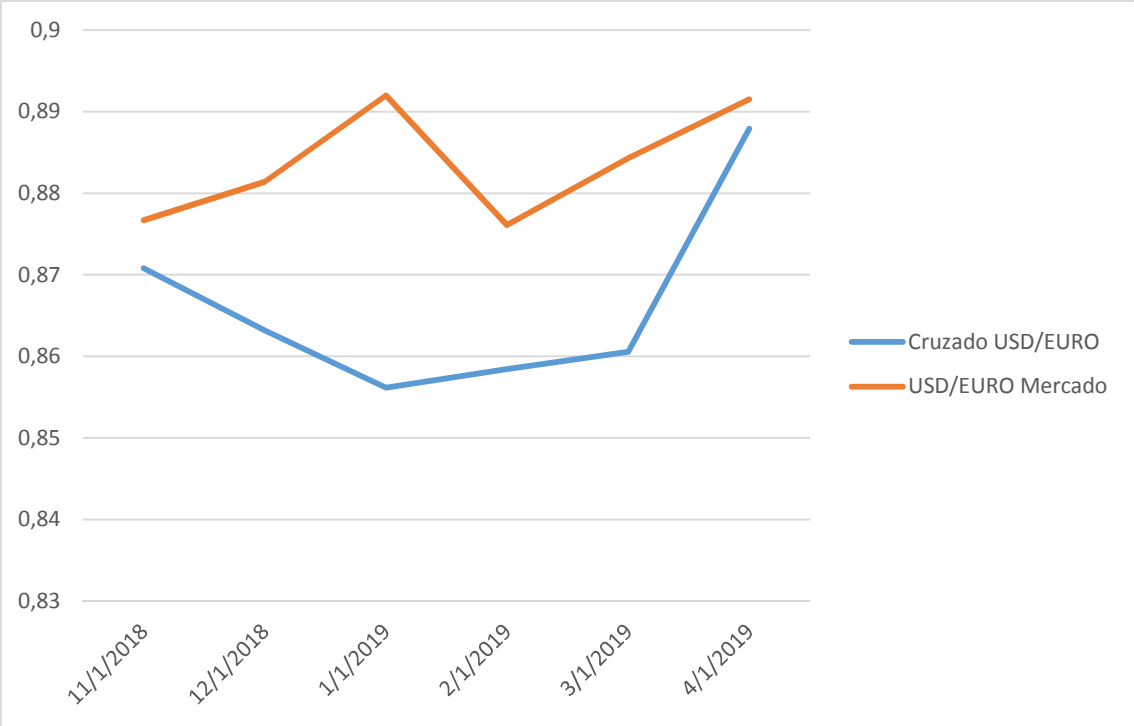


Figura 5.6 Ejemplo de precio donde hay arbitraje

Fuente: Elaboración Propia

Para comprender mejor la diferencia vamos a plantear un caso practico

[27] https://www.investing.com/

5.2.1 El Precio de Mercado se encuentra por encima del Precio Cruzado

Fecha	USD/BTC	EUR/BTC	Cruzado USD/EURO	USD/EURO Mercado
05/04/2019	0,000198	0,000223	0,887892377	0,8915
04/04/2019	0,000203	0,000229	0,886462882	0,8912
03/04/2019	0,000201	0,000226	0,889380531	0,8901
02/04/2019	0,000203	0,000229	0,886462882	0,8924
01/04/2019	0,000238	0,00027	0,881481481	0,8918
31/03/2019	0,00024	0,000274	0,875912409	0,891
30/03/2019	0,00024	0,000274	0,875912409	0,8914
29/03/2019	0,000239	0,000274	0,872262774	0,8905
28/03/2019	0,000244	0,00028	0,871428571	0,8893

Tabla 5.1 Cotización del Bitcoin en el mercado

Fuente: Investing.com

- Cambio de Dólar → Euro → Bitcoin

Iniciamos el ejemplo con un usuario que posee 100$ que quiere invertir. El usuario decide pasarlos a euros por lo que buscamos la cotización del día **05/04/2019**. Si miramos en la tabla vemos que el precio de mercado de ese día era **0,8915 USD/EUR** (el precio superior al cruzado 0,887892377 USD/EUR).

100 * 0,8915 = 89,15 €

El usuario ya tiene el dinero convertido en euros. A continuación, decide invertir en Bitcoin, por lo que tendremos que ver el valor de EUR/BTC, que ese día se encontraba en **0,000223 EUR/BTC.**

89,15 * 0,000223 = 0,01988045 BTC

Para concluir, el usuario decide hacer una nueva operación, de pasar los BTC a USD para poder analizar el resultado

0,01988045 * 0,000198 = 100,406313 $

Cómo se acaba de demostrar, el usuario tendría como resultado **100,406313$.**

100,406313 – 100 = 0,40631313 $

El usuario ha obtenido unas ganancias de **0,40631313$** fruto de la inversión realizada

- Cambio de Dólar → Bitcoin → Euro

A continuación, vamos a plantear el caso de antes, es decir, tenemos un usuario que posee 100$ que está interesado en invertir. La diferencia con el ejemplo anterior es el orden con el que se ejecuta los movimientos. La primera operación que realizamos es la adquisición de Bitcoin, para ello debemos mirar la cotización del día **05/04/2019** de USD/BTC, la cual es de **0,000198 USD/BTC.**

100 * 0,000198 = 0,0198 BTC

Continuamos con nuestro ejemplo pasando la cantidad obtenida a Euros, para la cual debemos fijarnos en que la cotización es de **0,000223 EUR/BTC.**

0,0198 / 0,000223 = 88,7892377 €

El ejemplo finaliza pasando nuevamente a dólares, para ello debemos fijarnos en el valor de mercado

88,7892377 / 0,8915 = 99,5953311 $

Una vez realizado todos los cambios del caso planteado, el usuario obtiene **99,5953311$**

100 – 99,5953311 = 0,40466891$

En este caso, el usuario ha perdido dinero, exactamente **0,40466891$.**

Con el ejemplo planteado anteriormente, acabamos de demostrar que el orden en el que se ejecute las operaciones afecta al resultado final monetario obtenido. Si el precio de mercado es superior al precio cruzado se consigue obtener rentabilidad pasando de Dólares a Euro y a continuación a Bitcoin. Si invertimos el orden, el resultado sería una pérdida.

Siempre y cuando el precio de mercado y el precio cruzado difieran obtendremos ganancias si realizamos la inversión con el orden Dólar, Euro, Bitcoin. Este hecho se puede utilizar para especular con el cambio de monedas y se puede producir arbitraje.

Si el precio cruzado hubiera estado por encima del precio mercado hubiéramos tenido pérdidas si se invirtiera en el orden que se plantea en el párrafo anterior y ganancias si el orden hubiera sido Dólar, Bitcoin, Euro.

CAPÍTULO 6: CONCLUSIONES

6.1 CONCLUSIONES

Como hemos visto a lo largo del trabajo la criptomoneda y sus diversos tipos son un producto que están modificando y renovando el mundo de las industrias y de una forma individual en los procesos de recolecta y administración de datos

Bitcoin nace en 2008 y comienza a ser minado en 2009. Sin embargo, como hemos puesto de manifiesto, su importancia en las transacciones es escasa hasta 2013.

De los primeros años de funcionamiento de Bitcoin, destacamos lo novedoso de la tecnología que incorpora (registros distribuidos). Aunque el número de transacciones es pequeño, el número de usuarios no ha dejado de crecer

A partir de 2013, sin embargo, comienza a aumentar el número de transacciones, se eleva el precio del valor y la capitalización de mercado. La importancia creciente hace que aparezca los primeros informes de las instituciones monetarias preocupados por la definición del valor, por la legalidad de las operaciones en las que se emplea y por su carácter especulativo

Se trata de un valor tremendamente volátil y por tanto de mucho riesgo como valor para la inversión.

En el momento actual, Bitcoin no representa una amenaza para monedas fuerte como el Euro o Dólar, pero si una alternativa para monedas muy débiles

En algunos países se está introduciendo determinada regulación a aquellas instituciones que operan con Bitcoin, a los operadores que hacen cambios entre monedas. Esto implica darle a Bitcoin un cierto estatus de moneda, pero también conlleva perder parte de su privacidad.

Este trabajo se ha centrado sobre todo en el Bitcoin y el Blockchain, los cuales ofrecen una gran cantidad de productos, servicios y formas de negocio. No obstante, la verdadera revolución recae en poder reducir los costes del sistema operativo y los de transacción.

Después del estudio realizado se puede afirmar que Bitcoin cuenta con unas series de características para ser una moneda descentralizada de bancos y entidades reguladoras

Bitcoin, cuenta con varias limitaciones con respecto al funcionamiento como moneda. Una de las limitaciones son las fluctuaciones que ha sufrido su precio como consecuencia de las especulaciones. Debido a estas fluctuaciones no se puede ver como un depósito de valor seguro y sin riesgo para los clientes. Otra consecuencia de las fluctuaciones es que cada vez se ve más como un activo financiero, es decir, una oportunidad de poder ganar dinero especulando.

Hay un tipo impositivo que está sujeto al uso de Bitcoin como moneda haciendo que el coste de la operación sea superior y favoreciendo que los usuarios usen el Bitcoin con fines especulativo en vez de con fines como moneda.

Para emplear Bitcoin como moneda se necesita contar con unas series de leyes que lo regulen y un sistema financiero que lo apoye, actualmente se encuentra en fase de inicio.

Bibliografía

Ali, R.;Barrdear,J.;Clews,R. y Shoutgate, J. (2014): The Economics of Digital Currencies, Bank of England, *Quaterly Bulletin*,2014 Q3, 276-286.

Autoridad Bancaria Europea (2014): Opinion on 'virtual currencies', disponible en https://www.eba.europa.eu/documents/10180/657547/eba-op-2014-08+opinion+on+virtual+currencies. pdf.

Andreessen, M. (2014) Why Bitcoin Matters. Publicado en The New York Time. En https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ . Consultado 13/03/2019

Arjona Brescolí, A. (2013). *La contabilidad triangular o de partida triple*. Editorial Club Universitario.

BBVA (s.f.): Historia de las Tarjetas de Crédito, en https://www.bbva.com/es/historia-de-las-tarjetas-de-credito/. Consultado 2/5/2019.

Dai, W. (1998): b-money, en http://weidai.com/bmoney.txt consultado el 22/05/2019

Down, K. (2014): New Private Monies: A Bit-Part Player? Institute of Economic Affairs Monographs, Hobart Paper 174. Disponible en SSRN: https://ssrn.com/abstract=2535299.

Escalona, S. B. e Inclán, L. V. (2012). Funciones resúmenes o hash. Revista Telemática, 10(1). En http://revistatelematica.cujae.edu.cu/index.php/tele/article/view/52

Espinach, P.C. y Ruzicka, T.F. (1999): *Costa Rica en el Mundo del Dinero Electrónico:Futura 3000 del BCIE*, Editorial Gala, San José (Costa Rica).

Banco Central Europeo (2012): *Virtual Currency Schemes*, en https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Galtés, M (2013). Bitcoin: De divisa misteriosa a burbuja financiera. Publicado en La Vanguardia, en https://www.lavanguardia.com/economia/20130407/54372214887/bitcoin-divisa-misteriosa-burbuja-financiera.html, consultado el 20/03/2019

Hayek, F.A. (1976); Denationalisation of Money, Hobart Papers 70, 2nd ed., The Institute of Economic Affairs, London.

Jiménez Gonzalo, C. y Tejero Sala, H. (2018): Cierre de Oficinas Bancarias y Acceso al Efectivo en España, *Revista de Estabilidad Financiera*, 34, 35-57.

Marín López, M.J. (2004): Las tarjetas de Crédito y el Artículo 15 de la Ley de Crédito al Consumo, *Revista de Derecho y Nuevas Tecnologías*, 5, 89-99.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Consultado el 18/02/2019

Navas Navarro, S. (2015). Un mercado financiero floreciente: el del dinero virtual no regulado (Especial atención a los BITCOINS). *Revista CESCO de Derecho de Consumo*, (13), 79-115.

Nieto Giménez-Montesinos, M.A y Hernáez Molera, J. (2019). Monedas Virtuales y Locales: Las Paramonedas, ¿Nuevas formas de Dinero? *Revista de Estabilidad Financiera*, Banco de España, 35,103-122.

Monzon, A. (2019) Criptomonedas: el futuro detrás de la burbuja. Publicado en El Independiente (25/5/2019), en https://www.elindependiente.com/economia/2019/05/25/criptomonedas-futuro-detras-burbuja/ consultado el 06/04/2019

Pérez, S (2018) La primera transacción con Bitcoin fue para comprar pizza. *Fortune.* En https://www.fortuneenespanol.com/tecnologia/historia-bitcoin-pizza-day-blockchain/ Consultado 15/05/2019 .

Plassaras, N. A. (2013). Regulating digital currencies: bringing Bitcoin within the reach of IMF. *Chicago Journal of International Law'l*, 14, 377-407.

Pastor, J (2018). Monederos físicos de bitcoin: qué son y cómo funcionan a la hora de proteger tus inversiones. Xataka. https://www.xataka.com/criptomonedas/monederos-fisicos-de-bitcoin-que-son-y-como-funcionan-a-la-hora-de-proteger-tus-inversiones Consultado 18/05/2019

Rivas Herazo, P.A. (2016): La Inclusión del Bitcoin en el Marco de la Soberanía Monetaria y la Supervisión por Riesgos en Colombia, *Revista de Derecho Privado*, 55, 1-36. En http://redalyc.org/articulo.oa?id=360046467006 Consultado 23/04/2019

Sarmiento, J., Garcés. J. (2016). Criptodivisas en el entorno global y su incidencia en Colombia. *Revista Lebret*, 8, pp. 151 – 171.

Smith, M (2009): Luca Pacioli: The Father of Accounting, disponible en SSRN: https://ssrn.com/abstract=2320658 or http://dx.doi.org/10.2139/ssrn.2320658

Torres Macias, E. M. (2015). *Reflexiones respecto a las ventajas y desventajas del uso del Bitcoin*, Bachelor's thesis, Universidad Piloto de Colombia. En http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/3750/00002077.pdf?sequence=1

Urrutia, c. (2016): Las compras con tarjeta superan por primera vez a las de efectivo, publicado en Diario el Mundo (2/7/2016), en https://www.elmundo.es/economia/2016/07/02/5776c55d22601d4a2d8b45d1.html

Vásquez Leiva, M. (2014). Bitcoin: ¿Moneda o burbuja? Revista Chilena de Economía y Sociedad, 8, 52-62.

Webgrafía

Banco Central Europeo, en https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.es.html, Consultada 11/04/2019.

Bitcoin organización: https://bitcoin.org/es/

Blockchain.info. en http://www.blockchain.com Consultado 26/05/2019

CoinMarketCap: https://coinmarketcap.com/es/ Consultado 03/05/2019

Criptonoticias. https://www.criptonoticias.com/ Consultado16/03/2019

Economía simple.net https://www.economiasimple.net/criptomonedas Consultado 06/03/2019

Economipedia Haciendo fácil la economía. https://economipedia.com/definiciones/bitcoin.html Consultado 27/04/2019

Elbitcoin.org. https://elbitcoin.org/strongcoin-bitcoin-seguro-y-al-alcance-de-todos/ Consultado 11/03/2019

FXstreet: https://www.fxstreet.es/ Consultado 29/05/2019

Investing.com. https://es.investing.com/crypto/bitcoin/btc-eur-historical-data Consultado 01/05/2019

GurusBlog. https://www.gurusblog.com/archives/historia-bitcoin/14/12/2013/4/ Consultado 21/05/2019

Obsevatorio Cetelem. https://elobservatoriocetelem.es Consultado 24/05/2019

Portalclientebancario, Banco de España. En https://clientebancario.bde.es/pcb/es/menuhorizontal/productosservici/serviciospago/Dinero_electronico.html Consultado 06/04/2019

Rankia. http://www.rankia.com/blog/divisas-y-forex/2082787-historia-bitcoin-como-evolucionado-estos-anos Consultado 15/04/2019

The Bitcoin Foundation https://bitcoinfoundation.org/

TradingView. https://es.tradingview.com/(17/04/2019)

Xataca. https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital Consultado 17/04/2019

Xavier Sala i Martín (Blog): http://salaimartin.com Consultado 03/04/2019

Zoomboomcrach, (2014, 04). La mejor explicación sobre qué es Bitcoin, la moneda virtual. *La información*. http://blogs.lainformacion.com/zoomboomcrash/2014/04/10/la-mejor-explicacion-sobre-que-es-bitcoin-la-moneda-virtual/ Consultado 04/03/2019

Anexos

Bitcoin: Se escribe con B mayúscula. Término empleado para designar la red, también es usado para referirse a un tipo de criptomoneda.

Bytes: Un byte en términos informáticos es una unidad de información que se usa en ordenadores y en telecomunicaciones. 1 Bit es 0,000001 Bitcoin.

Bloque: Unión de varias operaciones de Bitcoin que están esperando para ser verificadas y pasar a formar parte de una cadena de bloque. De media suele tardar unos 10 minutos en incorporarse un grupo de nuevas operaciones de Bitcoin a una cadena de bloque.

Bloque Génesis: Esta denominación se le atribuye a el primer bloque de una cadena de bloque.

BTC: Símbolo con el que se denomina el Bitcoin .

Cadena de Bloque: Podemos decir que es la contabilidad de la red Bitcoin. Consiste en una anotación de todas las operaciones realizadas con Bitcoin, de carácter público.

Clave Privada: Contraseña que reconoce el derecho de poder usar Bitcoin de una cartera Bitcoin a través de una firma criptográfica. Si usamos un monedero de escritorio las claves se guardarán en el ordenador. Si por el contrario, usamos un monedero web las claves se guardarán en un servidor del proveedor.

Clave Pública: Es más corta que la clave privada. Consiste en un texto de letras y números y es conocidos por todos. Podemos pensar que al ser algo conocido por todos cualquier usuario podría enviar Bitcoin a la dirección adjunta pero no es así, solo podrá hacerlo el que disponga de la clave privada.

Criptográfica: Técnica cuyo objetivo es ocultar los mensajes para que nadie excepto las personas autorizadas puedan entender dichos mensajes, en resumen, cuando decimos que algo está criptográfiado no es más que poner códigos a un mensaje para que nadie pueda leerlo excepto el destinatario.

Contabilidad Triple: A las cuentas de debe y haber se le añade una tercera cuenta que nos muestra los movimientos de flujo de efectivo. Esta cuenta está relacionada con los movimientos de flujo, que modificará el estado de flujo de efectivo.

Comisión: Cantidad de Bitcoin que se le entrega al minero a modo de recompensa como consecuencia de resolver un bloque.

Confirmación: Se da por confirmada una operación cuando el bloque ha sido resuelto y es casi seguro que no será revertido. La operación es incluida en la cadena de bloque.

Criptomoneda: Monedas digitales que permite los pagos digitales, la más conocida es el Bitcoin, aunque no es la única.

Criptografía: A través de las matemáticas se crean mensajes. Solo el destinatario puede entenderlo.

Deflación: Exceso de oferta produciendo una disminución en los precios y un incremento en el poder de compra.

Dirección: Es un identificador que posee de 27 a 34 caracteres de letras y números los cuales empiezan por el 1 o el 3. Su finalidad es recibir o enviar Bitcoin.

Doble Gasto: El efecto doble gasto se produce en el momento que un cliente de forma no muy correcta quiere desembolsar sus Bitcoin en dos usuarios distintos a la vez. La red Bitcoin ha sido preparada para que cuando se de esta situación se llegue a un acuerdo para decidir qué parte es verificada.

Firma Digital: Secuencia matemática que permite verificar la identidad del receptor, gracias a ello quien recibe el mensaje cuanta con los recursos suficientes para comprobar que el mensaje ha sido redactado por el emisor y no ha sido modificado por nadie más.

Hash: Podemos decir que el hash equivale a la huella dactilar, pues nos proporciona una identificación personal y única. De una forma más técnica definimos hash como un algoritmo matemático que nos proporciona una forma de identificarnos.

Inflación: Pérdida de valor de una moneda producido por la inestabilidad de la oferta y la demanda.

Minería: La acción de minar consiste en resolver los bloques verificando así que las transacciones que se contiene son correctas. Como recompensa los mineros reciben una pequeña cantidad de Bitcoin.

Monedero /Wallet: Espacio donde se almacena los Bitcoin. Podemos decir que es lo equivalente a una cartera física o a una cuenta bancaria en el banco. Los monederos poseen una clave privada.

P2P – Punto a Punto: El P2P hace referencia a un tipo de sistema que permite trabajar de un modo colectivo, es decir, los usuarios pueden comunicarse unos con otros de un modo directo. También permite realizar operaciones sin la presencia de un banco como intermediario.

Pool de Minería: Unión de mineros que se crea con el fin de obtener hash de una forma más veloz y aumentar así las probabilidades de descifrar el bloque y hacerse con la recompensa.

Satoshi Nakamoto: Nombre de un pseudónimo que hace referencia a la persona o grupo de personas que fueron los padres del Bitcoin.

Velocidad Hash: La velocidad hash es una unidad de medida que nos indica a que velocidad marcha la red Bitcoin. Si por ejemplo nos encontramos una velocidad hash de 12 TH/s quiere decir que la red está realizando 12 billones de cálculos en un segundo.

Volatilidad: Cambios que sufre una divisa con el paso del tiempo.