BITCOINS

Documentos electrónicos para el intercambio de bienes y servicios

LUIS ANTONIO GARCÍA ALEJO

bajo la dirección de

ÁNGEL LUIS SÁNCHEZ LÁZARO

UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

Trabajo de Fin de Grado

BITCOINS

Documentos electrónicos para el intercambio de bienes y servicios

Luis Antonio García Alejo

Ángel Luis Sánchez Lázaro

Salamanca, 2016

GARCÍA ALEJO, Luis Antonio

Bitcoin: Documentos electrónicos para el intercambio de bienes y servicios / Luis Antonio García Alejo; bajo la dirección de Ángel Luis Sánchez Lázaro – Salamanca: Universidad de Salamanca, Facultad de Traducción y Documentación, 2016. 65h

Trabajo de Fin de Grado – Grado en Información y Documentación.

1. Bitcoins. 2. Altcoins. 3. Criptografía. 4. Cadena de bloques. 5. Minería. 6. Web profunda. I. Sánchez Lázaro, Ángel Luis, dir.
II. Título

025

Resumen

Al hablar de Bitcoin no se hace alusión simplemente a una única cosa, al bien digital como tal, sino que nos referimos también al protocolo de envío y recepción de mensajes, basado en Open Source, a la red P2P (Par- a- par) y las propias criptomonedas (Bitcoins). Su creador, bajo el seudónimo de Satoshi Nakamoto, pretendía crear un proyecto con un objetivo principal: ***que las transacciones económicas entre dos personas no necesiten de un organismo central o ningún tipo de intermediario***. El objetivo de este estudio es explicar qué es el Bitcoin y las Criptomonedas, el contexto social y económico en el que surgieron y en el que se encuentran hoy en día, así como explicar cómo se crean y el uso que se hace de ellas (especialmente del Bitcoin) ya sea en el día a día, como forma de pago o intercambio de bienes, o como medio de inversión económica.

- **Palabras clave:** bitcoin, criptomonedas, altcoins, cadena de bloques, criptografía, dirección pública, clave privada, clave pública, monedero, intercambiador, red P2P, minería, web profunda.

Abstract

Speaking about Bitcoin one does not just simply refers to a single thing, the digital object, but we also refer to the protocol for sending and receiving messages, based on Open Source, to the P2P (Peer-to-peer) network and the cryptocurrency itself (bitcoins). Its creator, under the pseudonym Satoshi Nakamoto, intended to create a project with a main objective: ***that the economic transactions between two people do not require a central organism or any middle man***. The aim of this study is to explain what both Bitcoin and cryptocurrency are, their social and economic context, in which they arose and are today. I also want to explain how to create and use made of them, focusing on Bitcoin either in day to day, as payment or exchange for goods, or as a means of economic investment.

- **Keywords:** bitcoin, cryptocurrency, altcoins, blockchain, cryptography, public address, private key, public key, wallet, exchange, P2P network, mining, deep web.

SUMARIO

INDICE DE FIGURAS:

- **INTRODUCCIÓN:**

La motivación para realizar este estudio ha sido el interés por explicar que es el proyecto Bitcoin, contextualizar su aparición, así como el de las distintas criptomonedas surgidas a raíz de esta, establecer una relación entre la seguridad de la información y el Bitcoin, que exponga las principales ventajas y desventajas del uso de las nuevas tecnologías y características implementadas en este proyecto, analizar la relación que tiene con las instituciones, gobiernos centrales u otros organismos centrales y ubicarlo dentro de un marco legal así como analizar la situación del sistema monetario/bancario en la actual web 2.0 para realizar una comparación entre ambos y establecer unas conclusiones.

1. **Marco teórico:**

La aparición del dinero constituye uno de los grandes avances de la civilización humana en toda su historia.

Desde la antigüedad y antes de la aparición del dinero, las personas han intercambiado objetos de valor. Primero surgió el trueque, tras la necesidad de los individuos de adquirir bienes o servicios en posesión de otras personas. Se trata pues, de un intercambio de bienes o servicios por otros de un valor similar.

Siguiendo la evolución de la economía y a las nuevas necesidades, surgieron nuevos métodos de intercambio, y el valor que se le daba los objetos o servicios, por su propia utilidad, pasó a elementos u objetos con un simple valor simbólico o atractivo. Esto supuso el primer pasó hacía la creación del dinero y a lo largo de la historia han sido numerosos tipos de bienes los que se han "estandarizado" como medio de intercambio. Las características de estos bienes son: valor estable en el tiempo, disponibilidad, gran volumen, fáciles de almacenar y transportar, divisibles y no perecederos.

Fue entonces cuando surgió la asignación del dinero a metales preciosos como el oro, la plata o el bronce, pero este sistema en un principio presentaba dificultades para identificar su autenticidad, pureza y valor real, por lo que los gobiernos establecieron unos métodos de sellado, marcas y troquelado de las monedas de estos materiales preciosos, para asegurar su autenticidad. Así se crearon las primeras entidades reguladoras y los sistemas monetarios, y se crearon nuevas formas simbólicas de representar el dinero mediante el uso de papel y billetes, de los cuales su valor real o intrínseco es muy reducido en comparación con el valor que representan.

En el siglo XIX el dinero, físico (billetes y monedas) era respaldado por las entidades reguladoras por metales preciosos tales como el oro, plata o el bronce, de forma que

existía cierto "colchón" de seguridad a la hora de que una moneda se devaluara y de esta forma especificar mejor su valor. A esto se le denominó el Patrón oro (Paúl Gutierrez, s.f) que era el Sistema Monetario Internacional del Siglo XIX. Este Patrón oro comenzó a desaparecer en el siglo XX, debido a la Primera Guerra Mundial y posteriormente en 1971 de forma definitiva abandona el Patrón oro por parte de la por entonces sin duda primera potencia mundial EE.UU, para dar lugar al respaldo de la moneda solo por parte de la confianza que depositan los poseedores de la misma, este es el Sistema Monetario Internacional como se conoce hoy en día.

Esto ocasionó cierto impacto social y cambio de mentalidad de la sociedad, abriendo las puertas al mundo del dinero digitalizado, las tarjetas de crédito, etc.

En nuestra sociedad cada vez están más arraigados estos nuevos instrumentos de pago, sobre todos los basados en Internet, es decir herramientas que permitan a los usuarios comerciar por Internet de la manera más rápida y cómoda. Servicios ya asentados como PayPal o Google Wallet, ofrecen efectuar pagos sin necesidad de facilitar datos de cuentas bancarias o tarjetas de crédito. El Bitcoin es diferente al dinero digital o virtual que se tiene en una tarjeta de crédito o en una cuenta bancaria, ya que tal y como se conoce hoy en día, todo esto está centralizado y controlado por los bancos y los sistemas monetarios, en los cuales influyen directamente aspectos económicos, déficits de comercios, situaciones sociales, oferta y demanda etc. El Bitcoin surgió para crear un nuevo sistema económico y monetario con características y prototipos únicos, no conocidos hasta entonces.

1.1. El proyecto Bitcoin.

El autor del proyecto Satoshi Nakamoto difundió un artículo primigenio[1] explicando las características del proyecto y los métodos utilizados.

El Bitcoin, denominado por su creador (Satoshi Nakamoto, 2008) como una herramienta de pago Persona a Persona (en inglés *Peer to Peer: P2P*), está basado en un esquema de registro público global, formado por la comunidad de usuarios que lo utilizan, que opera de forma completamente descentralizada, y que cumple con determinadas características criptográficas, monetarias, logísticas y funcionales, que lo convierten en un mecanismo que puede considerarse como una moneda y constituir un gran salto en los medios de pago a escala global (Kleiman, 2013).

La información sobre la creación y uso del bitcoin, no se difundió de la manera más orgánica posible en sus comienzos, pese al artículo publicado por el autor, este era

[1] Artículo original escrito por el autor del Bitcoin, disponible en: https://bitcoin.org/bitcoin.pdf
Versión en español traducida por Breathingdog disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

entendido solo por los usuarios que entendían los aspectos técnicos sobre el tema. Su valor inicial era de apenas 0.00076 $ por bitcoin[2].Surgió en el contexto de plena crisis económica mundial y en un par de años se impulsó hacia un mayor conocimiento del proyecto por más usuarios. Debido a la incertidumbre sobre los sistemas bancarios nacionales, la apuesta por el bitcoin fue realmente fuerte, sobre todo a comienzos de 2014 cuando se produjo su gran auge.

Junto con un mayor proceso de difusión de información sobre el Bitcoin, surge cierta desinformación a los usuarios debido a la naturaleza del mismo debido a su vez, a los intereses que hay detrás por parte de las instituciones reguladoras y bancos centrales que, lógicamente por su parte, no están a favor del auge de una criptomoneda "invisible" en la cual no sean capaces de intervenir y controlarla, así como las actividades y el comercio que se realizan con ellas (elEconomista, 2013). Esto supone, junto con otros aspectos, que en los 2 últimos años la criptomoneda se haya devaluado significativamente y finalmente ha pasado a un valor más estable después del auge que supuso el *boom* de 2014.

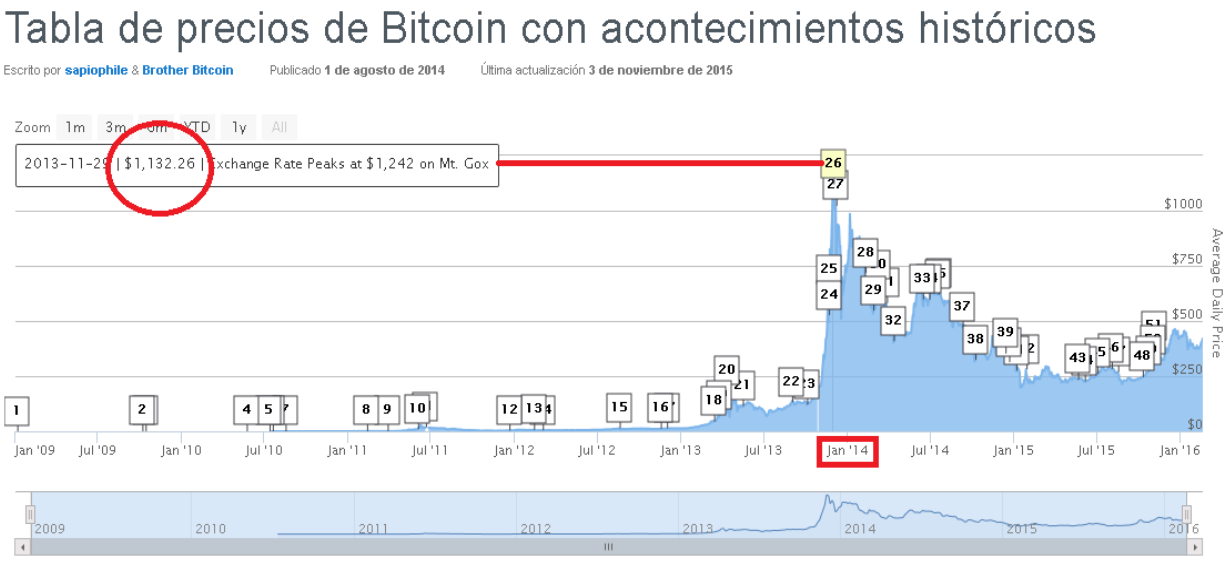


Figura 1.Datos de la mayor cotización histórica del Bitcoin (Bitcoin/Dólar Estadounidense)[3]

[2] Todos los datos sobre el valor y los acontecimientos históricos del Bitcoin disponibles en: https://bitcoinhelp.net/saber/m%C3%A1s/historia-del-gr%C3%A1fico-precio?lang=es

[3] Fuente: https://bitcoinhelp.net/saber/m%C3%A1s/historia-del-gr%C3%A1fico-precio?lang=es

2. Metodología:

Se ha considerado abarcar y contrastar datos, publicaciones, documentación y noticias ya existentes, para reflejar en este estudio de la forma más exacta posible el análisis de este tema y confrontar las problemáticas que surgen sobre aspectos legales, seguridad y mantenimiento de las criptomonedas.

Para establecer un flujo de noticias he utilizado la tecnología RSS de sindicación de contenido, en las secciones de tecnología de prensa digital, como El Economista, La Vanguardia, entre otros, que tratan el ámbito del Bitcoin o las criptomonedas. Debido a la naturaleza del tema, la actualización y evolución es constante y ha sido fundamental para la realización de este trabajo, estar informado de estos cambios.

Por otro lado para la búsqueda de información divulgativa o artículos previos realizados, se han consultado las bases de datos de Web of Science en búsqueda de artículos relacionados con el Bitcoin y las criptomonedas, dentro de los pocos artículos publicados (11 resultados en el caso de la búsqueda por tema "*Cryptocurrency"* y 61 resultados en el caso de la búsqueda *"Bitcoin")* algunos artículos con más relevancia publicados, han servido de referencia para realizar este trabajo. Para el contexto legal se han consultado también varios estudios ya publicados que especifican la situación en la que se encuentra el Bitcoin actualmente, como el publicado por Abanlex, un bufete de abogados con sede en Madrid especializado en derecho tecnológico y otro artículo publicado por The Law Library of Congress, con la situación del Bitcoin en distintos países del mundo.

Para la documentación más técnica y el análisis de datos estadísticos se han utilizado principalmente dos fuentes de información, entre otras, son: *Bitcoin.org*, la plataforma oficial de Bitcoin en Internet, y el mercado de capitalizaciones *Coinmarketcap*.

3. Contexto legal:

Legalmente el dinero es una representación abstracta de un valor (independiente del propio valor inherente al papel o al metal) respaldada por una autoridad y generalmente admitida para la realización de intercambios (Bernardo, 2013). La diferencia radica en que el dinero electrónico se intercambia por bits.

3.1. Legalidad del bitcoin en España:

En septiembre de 2012 se creó la fundación *Bitcoin Foundation*, una organización sin ánimo de lucro, a semejanza de otras como la Apache Software Foundation o la Linux Foundation, para estandarizar, proteger y promover el bitcoin, y mantenerlo fiel a sus principios fundamentales: **una economía que no dependa de la política, abierta e independiente.**

Desde el punto de vista jurídico es difícil ubicar el Bitcoin en la legalidad o no (Fernández Burgueño, 2013). Existen normativas creadas por la Unión Europea respecto al dinero electrónico, como la Directiva 2000/46/CE, que fue incorporada en España mediante la Ley 44/2002. Una actualización posterior se da con la Ley 21/2011, que especifica qué entidades pueden ser emisoras de dinero electrónico:

1. Entidades de crédito
2. Entidades de dinero electrónico autorizadas por el Ministerio de Economía y Hacienda
3. Sociedad Estatal de Correos y Telégrafos
4. Banco de España
5. Administración General del Estado, Comunidades Autónomas y Entidades locales.

En este contexto no se puede ubicar el Bitcoin, por lo que no se puede decir que el Bitcoin sea legal, sino "alegal". (Fernández Burgueño, 2013)

Desde un punto de vista jurídico no puede ser considerado como dinero electrónico al no contar con instituciones centrales que lo controlen (Jansen, 2012).

Pese a todo esto el Bitcoin no puede considerarse como ilegal, por lo general, en la mayoría de países occidentales, las autoridades no pueden suprimir su utilización. Los gobiernos trabajan para solventar los problemas derivados del uso de Bitcoins como el lavado de dinero (Luna,2015), el denominado mercado negro online (*deep web)* etc.

El bitcoin no es dinero electrónico (Fernández Burgueño, 2013):

- **El bitcoin no es dinero electrónico**, por así indicarlo la Ley 21/2011 (art.1.2).[4]
- **El bitcoin no forma parte del sistema monetario nacional**, por así indicarlo la Ley 46/1998 (art. 3.1).[5]

El bitcoin, como objeto de cambio, es legal, no es dinero, es un bien digital como pueden serlo monedas virtuales en un videojuego de rol.

"Un bitcoin es un bien patrimonial inmaterial, documento electrónico, objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada "Bitcoin", que permite ser utilizada como contraprestación en transacciones de todo tipo. Dichas unidades de cuenta son irrepetibles, no son susceptibles de copia y no necesitan intermediarios para su uso y disposición" (Fernández Burgueño, 2013).

Para obtener Bitcoins estos pueden conseguirse por medio del trueque (*"Cambio X cantidad de bitcoin por 1 coche / casa /…"*) y por medio de la minería, que se explica más a fondo en el apartado de Desarrollo.

Pagar con bitcoins es legal, el problema es que debido a su desconocimiento social y sobre todo el filo legal en el que se encuentra, hace que la gran mayoría comercios tanto online como físicos no acepten dicha criptomoneda como intercambio por sus bienes. Pese a ello, como ocurrió con PayPal y otros sistemas de pago electrónico en un comienzo poco a poco las empresas confían más en aceptar este medio de pago.

3.1.1 Normativa y facturación de bitcoins.

Afirmaciones según Fernández Burgueño sobre los cobros en bitcoins y la contabilidad de los mismos:

Es legal cobrar en bitcoins.

Cobrar en bitcoins es legal, como también lo es cobrar en objetos como muebles o zapatos.

Los pagos que se realizan en bitcoins son permutas, según indica el Código Civil (art. 1538):[6]

[4] http://noticias.juridicas.com/base_datos/Admin/l21-2011.html#a1
[5] http://noticias.juridicas.com/base_datos/Admin/l46-1998.html#c2s1

A efectos de contabilidad, la entrega de bitcoins a cambio de un producto o de una prestación es un canje de activos, que son naturalmente diferentes y que da lugar a una permuta de tipo comercial (Norma de Registro y Valoración 2ª 1.3 del RD 1514/2007).[7]

-Se puede llegar a conocer quién realiza una transferencia de bitcoin :

La asociación de un nombre de usuario a un cuenta se puede realizar e incluso llegar a conocer a la persona que está detrás, pese a la característica de no rastreabilidad de los usuarios de Bitcoin, si estos usuarios no han tenido la precaución de utilizar varias claves públicas (direcciones) en las transacciones o de desvincular su identidad con su cuenta de correo electrónico Bitcoin (en caso de utilizar los servicios online), con tiempo, se puede hacer un seguimiento, hasta el origen, de cada transacción.

-El bitcoin vale lo que estés dispuesto a pagar por él:

El valor del bitcoin fluctúa constantemente. El motivo es que un bitcoin vale lo que alguien esté dispuesto a pagar por él. Aunque en el mercado de esta criptomoneda se especule su valor real frente a monedas centralizadas como el dólar o el euro.

El comprador y el vendedor pueden negociar el precio y el tipo de moneda de cambio que quieran para un bitcoin, como el intercambio por otro tipo de criptomoneda, o pueden tomar alguna referencia del mercado, por ejemplo el cambio a dólares.

-Si se paga con bitcoins, se debe facturar.

El Bitcoin, considerado "servicio" a efectos fiscales, pueden venderse y adquirirse sin necesidad de que las partes firmen documento alguno.

Se produce el siguiente efecto para el que paga con bitcoins:

- La empresa que paga debe emitir una factura de venta de esos bitcoins**.** Así lo indica el RD 1619/2012 (art. 2)[8].
- El particular, que deberá ser mayor de edad o emancipado (art. 1263 del Código Civil)[9], debe ser capaz para realizar actos de venta de servicios. También pueden pagar con bitcoins otras personas menores de edad, siempre que se mantenga la capacidad y este acto de permuta esté conmunmente aceptado para los mismos.

[6] http://noticias.juridicas.com/base_datos/Vacatio/v0-cc.l4t5.html
[7] http://www.boe.es/boe/dias/2007/11/20/pdfs/C00001-00152.pdf
[8] http://www.boe.es/buscar/act.php?id=BOE-A-2012-14696
[9] http://noticias.juridicas.com/base_datos/Privado/cc.l4t2.html#a1263

En el caso de que el vendedor sea una persona física, la empresa que lo adquiere deberá aplicar el ITP (Impuesto sobre Transmisiones Patrimoniales Onerosas), regulado en el RDL 1/1993[10].

El bitcoin forma parte del patrimonio.

Desde un punto de vista contable, los bitcoins son bienes digitales y, al ser adquiridos por una empresa, incrementan su patrimonio**.** (Fernández Burgueño, 2013)

En nuestro país la adquisición de bitcoins está regulada en el RDL 1/1993. Esta norma indica que dicha adquisición es una operación sujeta y no exenta al Impuesto sobre Transmisiones Patrimoniales (ITP), que es diferente en cada comunidad autónoma. Por ejemplo, en Madrid y en Cataluña se debe pagar un 4% del valor de adquisición de los bitcoins.

Para conocer el precio de compra y de venta de bitcoins y hacer el cálculo correcto, la empresa deberá aplicar un método admitido en Derecho contable, como el PMP (precio medio ponderado), el FIFO (first in, first out) o el LIFO (last in, first out). (Fernández Burgueño, 2013)

El bitcoin no es un activo financiero.

En España, hoy, el bitcoin no se trata como un activo financiero**,** según indica el Plan General de Contabilidad (9ª norma de registro y valoración)[11].

Entre los activos financieros indicados en la norma (créditos, valores, acciones, fianzas, etc.) el que hace mención al "efectivo y otros activos líquidos equivalentes" puede causar alguna duda, que queda rápidamente despejada consultando la norma 9ª de elaboración de las cuentas anuales y el epígrafe B.VII del activo del balance.

El bitcoin no es:

- La tesorería depositada en la caja de la empresa.
- Depósitos bancarios a la vista.
- Instrumentos financieros que sean convertibles en efectivo y que en el momento de su adquisición, su vencimiento no fuera superior a tres meses, siempre que no exista riesgo significativo de cambios de valor y formen parte de la política de gestión normal de la tesorería de la empresa.

[10] http://noticias.juridicas.com/base_datos/Fiscal/rdleg1-1993.t1.html
[11] http://www.boe.es/boe/dias/2007/11/20/pdfs/C00001-00152.pdf

En cuanto a si el Bitcoin debe considerarse CFD (contrato por diferencia) (en inglés *Contract for Difference*). Los CFD son contratos que implican una obligación de cobro o de pago bajo condición. En el momento en que se conviene, se genera un pacto entre dos personas obligadas por el contrato aceptado. Sin embargo, el bitcoin, una vez adquirido, es un bien intangible que tributa como servicio y que no obliga, por sí solo, a uno mismo o a terceros, al pago o al cobro de cantidad alguna. Por tanto, no podría aplicarse la regulación de los CFD a los Bitcoin. (Fernández Burgueño, 2013)

Usar bitcoins es una actividad de riesgo

El valor del bitcoin es altamente volátil y podrías ganar dinero con él, mantenerlo o perderlo todo. Ya que se su fluctuación depende directamente de la oferta y demanda de los propios usuarios del bitcoin. (Fernández Burgueño, 2013)

3.2. Situación legal del bitcoin en algunos países.

En la mayoría de países de Hispanoamérica, África y Oriente medio, el bitcoin se marca como desconocido, mientras que en Estados Unidos, Canadá y Australia su uso es completamente permisivo (Tobar, 2014). En el mapa se identifica que en Tailandia[12] e Islandia su situación es ilegal (Mirando, 2013).

[12] Tailandia se convirtió en el primer país en prohibir el uso del Bitcoin. Acceso a la noticia completa: https://www.fayerwayer.com/2013/07/tailandia-es-el-primer-pais-en-prohibir-el-uso-de-bitcoin/

Figura 2. Mapa interactivo de la situación legal del Bitcoin en el mundo.[13]

Colores:

- Verde: permisivo
- Amarillo: conflictivo
- Rojo: hostil
- Gris: desconocido

Como se puede observar en el mapa se refleja cómo en el mundo occidental y en Australia el bitcoin puede ser utilizado como bien o servicio. Al contrario en toda Rusia y oriente el uso es más restrictivo incluso está prohibido como es en el caso de Japón.

Es conveniente resaltar el caso de Japón, que no aparece en el mapa, en el cual el bitcoin está actualmente desacreditado (Pérez Rodríguez, 2015).

3.2.1. Países y territorios específicos:

En este apartado se presenta un resumen de la situación legal del bitcoin en distintas zonas del mundo (The Law Library of Congress, 2014):

-Estados Unidos:

Estados Unidos considerará a efectos fiscales el bitcoin y otras monedas virtuales como propiedad intangible y no como divisa, por lo que estará sujeta a impuestos.

-Argentina:
Según la Constitución Nacional de Argentina la única autoridad capaz de emitir monedas de curso legal es el Banco Central, por lo tanto el Bitcoin no se considera moneda legal en curso, pero sí se puede llegar a considerar dinero aunque no se puede utilizar para pagar deudas u obligaciones, pero sí, como señalan algunos expertos, pueden considerarse un bien y pueden regirse por las reglas de venta de mercancías en el Código Civil como un bien de intercambio o "cosa".

-Australia:
En 2013 la *Australian Taxation Office* (ATO) Oficina de Impuestos Australiana reveló para un artículo de la Australian Financial Review que estaba en supervisión del Bitcoin y de todos los aspectos relacionados con su volatilidad, evolución e interacción con otras monedas, así como en el mismo artículo se pone de manifiesto la intención por parte del gobierno australiano de ejercer un control y establecer los mismos requisitos fiscales y de control sobre esta criptomoneda que con otras monedas ya centralizadas.

[13] La situación legal del Bitcoin en un mapa interactivo. [en línea] Disponible en: http://www.maestrosdelweb.com/bitcoin-mapa-interactivo/ [Consultado el 5 mayo de 2015].

-China:
El 3 de diciembre de 2013, el banco central de China y otros cuatro ministerios centrales junto con otras comisiones emitieron conjuntamente un aviso sobre los riesgos del Bitcoin:

Definiéndolo como una "mercancía virtual", el aviso expresa que por la naturaleza el bitcoin, no puede considerarse como una moneda y no debe circular como tal ni ser utilizada en el mercado como una moneda. Lista de prohibiciones:

1. Los bancos y las entidades de pago en China tienen prohibido tratar con Bitcoins. Las instituciones financieras y de pago no podrán utilizarla fijación de precios para Bitcoin tratarlos como productos o servicios, comprar o vender bitcoins,o proporcionar directa o indirectamente Bitcoins.
2. Servicios a clientes, incluyendo: el registro, negociación, liquidación, compensación u otros servicios.
3. Aceptar Bitcoins o usar bitcoins como una herramienta de intercambio de información, y/o comerciar con bitcoins en China o en el extranjero.

El aviso promulga que es necesario seguir fortaleciendo la vigilancia de sitios de Internet que proporcionan bitcoins, su registro, el comercio y otros servicios. También advirtió sobre los riesgos de usar el Bitcoin como sistema para el lavado de dinero.

-Unión Europea:

La Unión Europea (UE) no ha aprobado ninguna legislación específica en relación con el estado del bitcoin como moneda. En octubre de 2012, el Banco Central Europeo publicó un informe sobre la moneda virtual. Publicó una serie de esquemas que analiza el sistema de Bitcoin y brevemente analiza el estatus legal bajo la ley de la UE.

Algunos expertos sugieren que la red del bitcoin puede entrar dentro de la definición de la Directiva sobre el dinero electrónico 2009/110 / CE.

Dicha Directiva define el dinero electrónico basado en tres criterios:
(a) De almacenamiento electrónico.
(b) La emisión a la recepción de los fondos.
(c)Aceptación como medio de pago por una persona física o jurídica distinta del emisor.

El informe establece que el bitcoin reúne el primer y tercer criterio, pero no el segundo. Otros expertos sugieren que el bitcoin entra dentro de la definición de Directiva de Pago de Servicios 2007/64 / CE. (The Law Library of Congress, 2014)

En general, la presente Directiva establece normas relativas a la ejecución de pagos a través del dinero electrónico. Sin embargo, como concluye el informe, el bitcoin queda fuera del ámbito de aplicación de la Directiva2007/64 / CE, ya que la presente Directiva no se ocupa de dinero electrónico y porque las instituciones incluidas por la directiva no están autorizadas a emitir dinero electrónico.

-India:

No parece haber ningún marco legal explícito que regule, restringa o prohíbabitcoins en la India.
Sin embargo, el banco central de la India recientemente advirtió públicamente de los posibles riesgos de ataques de ciber seguridad y lavado de dinero relacionados con el uso de estas monedas virtuales. En24 de diciembre 2013, el Banco de Reserva de India RBI (Reserve Bank of India) emitió un aviso público a los usuarios, titulares y los comerciantes de monedas virtuales (VC), incluidos Bitcoins , en relación con el potencial riesgo financiero, la legalidad del mismo, protección de la clientela que opera con ellos y los riesgos de seguridad relacionados que están exponiéndose a sí mismos.

-Israel:

Según informes de prensa, los funcionarios del Ministerio de Justicia y Bank of Israel han tenido como fuente de debate las implicaciones del uso de bitcoins, en particular en transacciones ilícitas.
Los activistas israelíes pro bitcoin destacan las ventajas de utilizar la moneda virtual, mientras que los expertos sostienen, debido a la fluctuación del precio actual que los bitcoins que "no son depósitos fiables de valor", una característica importante de la moneda es que funciona de forma anónima, lo cual es un atractivo para las transacciones ilícitas ocasionando un problema en la supervisión del gobierno que no pueda ser capaz de controlarlo.

-Rusia:

De acuerdo con un informe elaborado por el bufete de abogados de Rusia *Tolkachev and Partners*, en la actualidad no hay hechos jurídicos que regulen específicamente el uso de bitcoins en la Federación Rusa.

Sin embargo, el uso de bitcoins puede ser restringido, teniendo en cuenta el artículo 140 del Código Civil de Rusia, que reconoce el rublo ruso como el medio exclusivo de pago en la Federación Rusa y requiere que todos los precios de las transacciones financieras realizadas en Rusia se definirán en rublos.

De acuerdo con el informe, si el bitcoin es considerado como una moneda extranjera a los efectos de una transacción en particular, tal transacción puede ser reconocida como una operación de divisas ilegales sujeta a enjuiciamiento en virtud de la ley Rusa de responsabilidad administrativa.

German Gref, presidente del mayor banco del gobierno ruso (Sberbank), declaró, que las autoridades rusas están monitorizando los acontecimientos relacionados con el bitcoin, como ya ocurre por ejemplo en Australia

También declaró que la regulación mundial en las monedas virtuales será necesitará en un futuro cercano, e incluía a Rusia como parte de este proceso de regulación. Además, dijo que la emisión de moneda virtual puede iniciarse en Rusia basado en los sistemas de pago en línea nacionales ya existentes.

-Corea del Sur:

En la actualidad no hay leyes en Corea del Sur respecto a la regulación del uso de Bitcoins.
Sin embargo, el presidente del Banco de Corea recomendaba en una rueda de prensa en diciembre de2013, que el bitcoin debe ser regulado en un futuro.

3.3. *Deep web* (Internet profundo).

El Bitcoin se caracteriza por el anonimato, el difícil rastreo y seguimiento de las personas que están detrás de las transacciones que se realizan con él (Tecayehuatl, 2013)

Por ello las principales ventajas de esta criptomoneda se convierten en su mayor debilidad a ojos de la población ya que al no estar regulada ni centralizada por ninguna entidad o estado su uso es escaso en comparación con una moneda corriente fiduciaria e incluso las criptomonedas son relacionadas a menudo con el mercado negro y más en concreto en la famosa "*deep web*". (Caffyn, 2015)

Para entender mejor estos aspectos se define que se considera web superficial y que se considera *deep web*:

Web superficial es a la que se accede mediante las consultas a buscadores, y que se basan en relaciones existentes entre un sitio y los hipervínculos que alberga, así surgió el término navegar por la web, ya que se va de una página a otra, debido a la interrelación directa con cada sitio indexado en un buscador (Becerra Gutiérrez, 2014).

La ***deep web*** es una porción muy extensa de Internet *(se estima que alrededor del 90% de Internet)* que queda invisible e inaccesible a tecnologías de indexado y rastreo web

(Google, Yahoo, Bing, etc). A ella solo se puede acceder a través de una consulta exacta dentro del contenido de alguna base de datos (Becerra Gutiérrez, 2014).

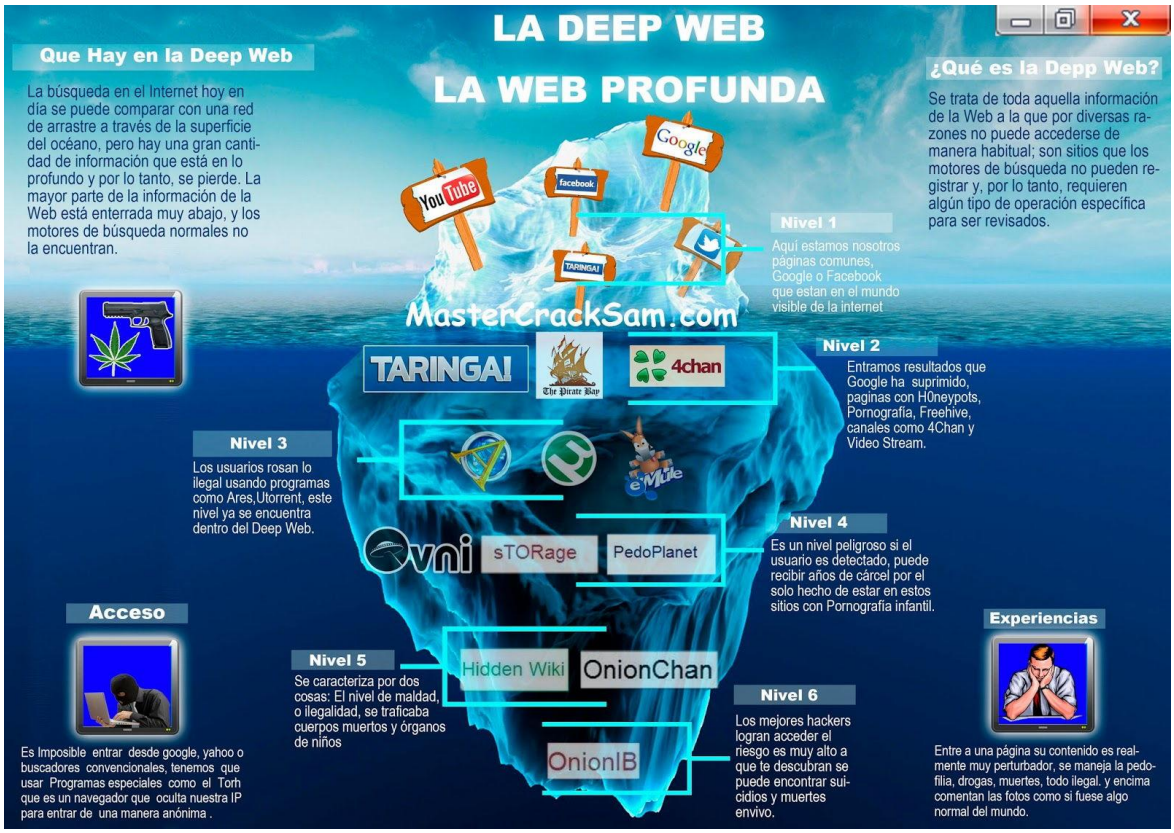


Figura 3. Esquema de los distintos niveles de la deep web[14]

Las siguientes características hacen que cualquier tipo de archivo o sitio web pertenezca a la deep web, debido a que no ha sido indexado (Becerra Gutiérrez, 2014):

1. Tener mecanismos que fallen, mal diseño o interfaces que interfieran con los *bots*[15] de los buscadores.
2. Contenido aislado. La página web no tiene enlaces, ni referencias a otras páginas web, al mismo tiempo que ningún sitio web hace referencia ni enlaza la página aislada.
3. Subdirectorios o bases de datos con acceso restringido
4. Contenidos no basados en HTML o que están codificados.
5. El contenido está protegido por contraseña o cifrado

[14] Imagen proporcionada por Finterocaso. Artículo completo disponible en: https://myopiniones.wordpress.com/2015/04/20/deep-web-internet-profunda/

[15] Bots *(del inglés Robot),* es el contexto de los buscadores, es una herramienta programada que inspecciona todas las páginas del World Wide Web (WWW), para el procesado posterior de un motor de búsqueda que las indexa, proporcionando un sistema de búsqueda rápido. Fuente: https://es.wikipedia.org/wiki/Ara%C3%B1a_web

Dentro de la web profunda, hay contenidos especialmente diseñados para permanecer ocultos o ubicarse en distintas capas separadas de las capas públicas de Internet (Becerra Gutiérrez, 2014).

Las redes virtuales privadas (*virtual private networks* o VPN) son tecnologías que se clasifican como web profunda y es ahí donde se hace principalmente el uso de las mismas. Estas redes tienen una infraestructura y contenidos a los que solo se puede acceder a través de un software específico, entre los más destacados se encuentra TOR, del cual se detalla qué es y su funcionalidad a continuación:

Tor de las siglas "*The Onion Router"* o enrutamiento de cebolla, es un proyecto diseñado y creado por la marina de los Estados Unidos, que actualmente está en manos de la organización sin ánimo de lucro "Tor Proyect" que tiene como objetivo que millones de personas en el mundo tengan libertad de acceso y expresión en Internet manteniendo su anonimato y privacidad.

Tor funciona como una red de túneles virtuales que permite a los usuarios navegar con privacidad, a los desarrolladores les permite crear aplicaciones para el intercambio de información sobre redes públicas sin tener que comprometer su identidad, permite eliminar el rastreo que hacen numerosos sitios web de los hábitos de navegación, y permite publicar sitios webs sin revelar la localización del creador.

Estas características y para este uso fue diseñado el proyecto, pero debido a su confidencialidad y privacidad, en ocasiones, el uso que se hace de esta tecnología de red de anonimato es como refugio y como red de actividades ilegales, llegando incluso a ser Tor sinónimo de *dark web* o mercado negro.

Su uso puede ser benevolente o delictivo, para mantener actividades ilícitas (tráfico de armas, mercado de drogas, lavado de dinero, terrorismo), por lo tanto es declarado abiertamente por numerosas agencias gubernamentales que la *deep web* se considera el refugio de delincuentes.

No se conoce exactamente la evolución ni el crecimiento de la web profunda a lo largo de los años, pero la aparición del Bitcoin marcó sin duda un antes y un después, debido a sus características junto con las que ofrecen tecnologías como Tor han supuesto en el ámbito criminal la optimización de los medios pago y el anonimato de las transacciones.

Este, sumado a otros muchos factores, influyen claramente en las decisiones que los gobiernos puedan tomar respecto a la legalidad de la criptomoneda y es otro incentivo por el cual todavía no existe una regulación clara y precisa y conlleva que la criptomoneda se encuentre hoy en día en una especie de "limbo" legal (Kristoufek, 2013).

4. Panorama ALTCOINS:

4.1. Comparativa: Bitcoin vs Altcoins.

Con la aparición del Bitcoin, son numerosos los usuarios o las comunidades que ven como un proyecto de futuro sólido e innovador, el sistema económico planteado por esta criptomoneda. Es por esto que tras la experiencia y gracias a la característica de Código abierto del Bitcoin bajo licencia MIT(**Massachusetts Institute of Technology),** lo que permite un estudio y análisis más profundo de su funcionamiento**,** los usuarios, deciden llevar a cabo su propio proyecto de criptomoneda, creando otro tipo de moneda criptográfica con unos prototipos comunes que comparten con el Bitcoin, pero incluso añadiendo modificaciones, nuevos algoritmos, nuevos métodos de minería (obtención de criptomonedas a través de recursos informáticos físicos) y objetivos o metas para su criptomoneda.

Es así como surgen los denominados Altcoins o monedas alternativas que son una variante del Bitcoin, con sus propios precios de mercado establecidos y su regulación por parte de la comunidad de usuarios que lo controla.

Sobre todo en los últimos años estos Altcoins han ido cobrando fuerza e incluso algunos proyectos decriptomonedas, se han convertido en competidores directos de la criptomoneda por excelencia, el Bitcoin.

Hoy en día los factores que influyen en la decisión por parte de un usuario que desea adentrarse en el mundo de las criptomonedas, comparten una similitud en la decisión que toma una persona por usar un tipo de moneda centralizada u otra, como el dólar, la libra o el euro.

Estas similitudes son:

1. La situación geográfica:

   Principalmente en el caso de las monedas centralizadas es claramente influyente pero en el caso de las criptomonedas lo es también, aunque sea a menor escala, ya que si por ejemplo en una determinada comunidad, país, sociedad es más común el uso de un tipo de moneda criptográfica tú te verás influenciado para el uso de la misma.

2. El contexto social y la confianza en la moneda:

   El uso que se pueda llegar a hacer de la criptomoneda en tu entorno, los aspectos de seguridad que te ofrece distintos de los proyectos ya creados, y en definitiva que no se quede sin uso, que no sean proyectos volátiles, de prueba, o de fraude

por parte de algunos usuarios que a través del desconocimiento y la desinformación que hay sobre esta temática, aprovechan para engañar y dañar la imagen que se tiene de la comunidad de usuarios de estas criptomonedas.

3. La accesibilidad a la información y comunidad de usuarios:

Es importante a la hora de decidir que criptomoneda utilizar,que el proyecto que se quiere llevar a cabo de la criptomoneda, esté bien definido con los objetivos planteados y la facilidad que encuentre el usuario en manejarse en la red de mercados, incluyendo transacciones, sea lo más intuitiva posible, adecuada al nivel de conocimientos del tipo de persona que pueda acceder a ella. Por ello dependiendo de la información que se encuentre sobre el proyecto, las noticias que surjan de la determinada criptomoneda, las opiniones de usuarios que la utilizan o la han utilizado, su reputación, etc.

4. Las necesidades particulares del usuario:

Las cuales son individuales y varían desde los objetivos que se tengan planteados, hasta los gustos propios.

4.2. Principales Altcoins.

En el siguiente apartado se recogen algunas de las principales Altcoins conocidas hoy en día, que más compiten con el Bitcoin, pero también he añadido ciertos proyectos de Altcoins que se están llevando a cabo que me parecen curiosos y oportunos de mención.

Existe un mapa[16] interactivo en Internet con la historia de todas las criptomonedas derivadas del Bitcoin, conocidas hasta la fecha, con opciones de búsqueda avanzada por tipo de algoritmo que utilizan, las que están operativas y las que ya han desaparecido.

Principales Altcoins, ordenadas por mayor valor de capitalización[17]:

[16] Mapa con datos de las criptomonedas disponible en: http://mapofcoins.com/bitcoin
[17] Los datos de capitalización, precio por unidad de moneda y total de monedas en circulación pueden variar y todos han sido consultados el día 22/02/2016 desde la página: https://coinmarketcap.com/

4.2.1. Ethereum.

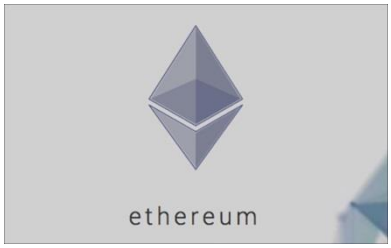


Figura 4. Logo de Ethereum.

Ethereum es el proyecto que se llevó a cabo por Gavin Wood, Jeffrey Wilcke, heikoheiko, a principios de 2014, con el fin de realizar todo tipo de acciones relacionadas con los intercambios financieros el "crowfunding" (financiación colectiva), propiedad intelectual, entre otras, y además que cualquier desarrollador cree y publique aplicaciones, utilizando esta plataforma orientada al Código abierto. La principal diferencia y lo que hace especial a este proyecto es que no se trata solo de la creación de una criptomoneda sino que abarca toda una red que tiene como objetivo la realización de todas las actividades mencionadas anteriormente, relacionadas con la filosofía del Código abierto.

El propósito inicial del proyecto Ethereum es el de "descentralizar la web" mediante la introducción de cuatro componentes como parte de los objetivos de su Web 3.0:

1. Publicación de contenido estático.
2. Mensajes dinámicos.
3. Transacciones confiables.
4. Interfaz de usuario integrada y funcional. Estos componentes están diseñados para remplazar algunos aspectos de la experiencia Web que se dan por sentado actualmente, pero haciéndolo de una manera completamente descentralizada y anónima.

Todas las actividades, transacciones y contratos se realizan con la criptomoneda descentralizada creada por estos mismos desarrolladores, denominada **Ether,** se fundamenta en un sistema de cadenas de bloques (*blockchain*), que permite a todos los usuarios controlar en tiempo real el valor de las operaciones realizadas, lo que en teoría dificultaría la especulación al estar monitorizadas globalmente y al mismo tiempo no hallarse sujetas al control por parte de ninguna entidad.

Por otro lado permite también un sistema de minería, como el existente en Bitcoin (que se explicará más a fondo en el apartado de desarrollo), pero que básicamente recompensa a los usuarios que cedan los recursos de hardware de sus equipos para

realizar las operaciones y transacciones que se llevan a cabo dentro de la red, con cierta cantidad de monedas, en este caso con Ether.

El proyecto en sus inicios fue bien acogido, ya que en las primeras 20 horas tras su lanzamiento, los primeros inversores compraron divisas de esta moneda por valor de 2,6 millones de dólares y hoy en día se consolida como un competidor directo del Bitcoin.

La capitalización actual de Ether es de 344,278,723$, con un precio por unidad de 4.46 $/ETH y un total de 77,202,405 ETH(Ether) en circulación.

4.2.2. Ripple.

Figura 5. Logo de Ripple.

Ripple es un producto de la empresa RippleLabs de EE.UU. RippleLabs es manejada por algunas de las mentes más brillantes del Silicon Valley, y financiado por los mejores fondos de los Estados Unidos, incluyendo Google Ventures, AndreesenHorowitz, etc.

Ripple es un sistema de pagos internacional multimoneda. Ripple se basa en algunos de los principios de Bitcoin, como ser el uso de una base de datos distribuida P2P (par a par).

Su fundamento es descentralizar las operaciones bancarias, y actividades de pago, por lo que en los bancos que implanten el sistema se encontrarían una serie de ventajas como: la reducción de los costes operativos en las transacciones de capital, reducir los tiempos de ejecución y liquidación de las operaciones y ofrecer nuevos servicios para los pagos mundiales.

Cada nodo de la red P2P de Ripple funciona como un sistema de cambio local y el capital financiero se sustenta en un capital social es decir, a través de la confianza entre las personas.

Entre sus propósitos busca la enrutación de los pagos a través de redes de ordenadores de confianza, abiertas y arbitrarias, de manera similar a como Internet enruta los paquetes de datos a través de dichas redes de ordenadores.

Con este objetivo Ripple se propone ser como una extensión o variante del sistema jerárquico o en rama bancario actual, en el cual los bancos son intermediarios entre sus clientes, y a la vez los bancos centrales son intermediarios de los bancos. Este sistema ocasiona potencialmente la aparición de puntos de fallo, en los que si un componente del sistema falla ocasiona un fallo en el sistema global.

La versión de este sistema que el proyecto Ripple quiere crear, es un sistema en el que una institución no controle ni tome las decisiones respecto a la política monetaria de toda una nación. Por el contrario todos los participantes de forma democrática decidirían el curso de la misma. A diferencia de pagos alternativos como PayPal que se mencionan en la introducción, Ripple se difiere en que, estos sistemas de pago digitales alternativos, tienen una autoridad central detrás, a través de la cual se dirigen sus políticas, y se encarga realmente de realizar los pagos y validar las transacciones entre los nodos de la red. En Ripple los nodos están descentralizados y no dependen de ningún control principal.

La moneda nativa de este proyecto es denominada XRP, y cumple las siguientes características:

1. Los XRP funcionan de "puentes" entre las monedas fiduciarias y las digitales. Complementan al Bitcoin en cuanto a la facilidad de intercambio de dinero fiduciario por criptomonedas, o por otro tipo de monedas.
2. Bitcoin es una criptomoneda descentralizada, Ripple es una red de transacciones descentralizada que **también** tiene una criptomoneda, lo cual no es obligatorio la posesión de ésta, para participar en la red.
3. En un principio, no existen costes de transacción. El coste de transacción para un usuario normal es minúsculo y no le afectaría prácticamente, se retiene una pequeña cantidad de XRP para que usuarios que intenten abusar con gran cantidad de transacciones del sistema, vean sus fondos rápidamente disminuidos.
4. **Los XRP no pueden minarse**, a diferencia de los Bitcoin, las transferencias no funcionan a través de un método de proof-of-work (prueba de trabajo), sino que Ripple funciona con el método de *proceso de consenso iterativo*[18]el cual no posibilita la minería. Se crearon 100 mil millones de XRP, los cuales no todos están en circulación ni disponibles a todos los usuarios sino que fueron divididos en distintas cantidades, 20 mil millones para los fundadores, 30 mil millones para OpenCoin, la "*startup*"(empresa emergente) que desarrolló Ripple, y 50 mil millones para promover Ripple y la circulación al público.

[18] Proceso de consenso iterativo: proceso a través del cual los nodos de la red comparten información acerca de las transacciones candidatas. A través de este proceso, la validación de los nodos se acepta en un subconjunto de transacciones candidatas para considerarlas en el libro de registro de transacciones.

Pretendían hacer la distribución lo más amplia, equitativa y justa posible, pero como toda empresa buscan un fin lucrativao y al igual que en el comienzo del Bitcoin, los creadores se quedan con una parte.

La capitalización actual de Ripple es de **276,358,087 $,** con un precio de 0.008107$/XRP y un total de 34,090,841,338 XRP en circulación.

4.2.3. Litecoin.

Figura 6. Logo de litecoin.

Litecoin es un criptomoneda lanzada en octubre de 2011 por un, entonces empleado de Google, Charles Lee, actualmente trabajando para CoinBase, una plataforma para el intercambios de Bitcoins. Se desarrolló como un proyecto similar al Bitcoin, criptomoneda descentralizada, sustentada por la red P2P, transferencias a través del sistema proof-of-work(prueba de trabajo) de código abierto bajo licencia MIT(*Massachusetts Institute of Technology),* pero con 3 principales diferencias con respecto al Bitcoin:

1. El tiempo de transacción de bloques en Litecoin es de 2,5 minutos con respecto a 10 minutos en Bitcoin, lo cual permite una confirmación más rápida de las transacciones, pero los expertos aseguran que con el riesgo de que sean menos seguras.
2. Los límites de emisión son diferentes en ambas criptomonedas. El máximo de emisión de criptomonedas para Bitcoin es de 21 millones frente a los 84 millones de Litecoin.
3. Algoritmo **Scrypt**: distinto algoritmo de funciones “hash” para sus transferencias a través de pruebas de trabajo. El de Bitcoin se denomina SHA-256.
4. La minería cambia al cambiar el algoritmo para resolver las transacciones, y estas al ser más rápidas con Litecoin, facilitan que equipos con menos recursos puedan realizar esta actividad. En un principio esto se vio como una ventaja de Litecoin frente al Bitcoin, pero en realidad la competencia tecnológica es lo que ha hecho crecer al Bitcoin frente a sus competidores, ya que se trata de una actividad de gran importancia en el sector y en la cual los competidores invierten grandes cantidades de recursos y energía.

5. Por último el proyecto Litecoin ofrece una interfaz de usuario distinta.

   La capitalización actual de Litecoin es de 154,649,393 $, con un precio de 3.47$/LTC y un total de 44,596,851 LTC en irculación.

4.2.4. Dogecoin.

Otro proyecto que **toma las bases de la bitcoin e inventa una critpomoneda** usando el mismo mecanismo y cambiando algunos aspectos que la han distinguido de las demás y la han hecho que el proyecto sea de las Altcoins más importantes.

Dogecoin es una criptomoneda que derivada del Litecoin, la cual deriva a su vez del Bitcoin. Fue creada por Billy Markus, como una moneda experimental partiendo del uso de otra criptomoneda denominada Bells. El logo y el nombre de Dogecoin provienen del "meme"(parodia de Internet) que tiene como imagen un perro de raza *ShibaInu*de origen japonés.

Figura 7. Logo de Dogecoin

El proyecto obtuvo popularidad, sobre todo en las redes sociales y especialmente en Twitter por lo que sus desarrolladores deciden implicarse más en el proyecto y lanzarlo y veían una oportunidad ganar números usuarios con respecto al Bitcoin, sobre todo debido a la reputación que tiene este último sobre el uso en el "Silk Road" o Internet profundo.

Existen varias opciones para conseguir Dogecoins (DOGE):

1. Al participar en la comunidad de Dogecoin: utilizan como plataforma principal la red social Reddit los usuarios pueden dar propinas a otros usuarios nuevos, que realicen alguna "buena acción" en Internet. Una característica de la comunidad de Dogecoin es la participación activa y que no se toma en serio a sí misma, su origen como forma de parodia y experimento, no busca

enriquecerse a través de este proyecto sino que es una participación de usuarios más o menos altruista.

2. Registrarse en un "faucet": que son sitios web que ofrecen una pequeña cantidad de Dogecoin gratuitos para que los usuarios se inicien en el uso de esta criptomoneda.
3. Comprar directamente Dogecoins por dinero corriente en cualquiera de sus mercados. Los mercadores que se recomiendan a través de su página web oficial son:
    a. WellSellDoge
    b. ANXPRO
    c. Celery
4. La minería. Actualmente ya se han minado más del 80% del total de Dogecoin (100 mil millones). Al igual que Litecoin, **Dogecoin utiliza el algoritmo scrypt** para realizar las transacciones a través de pruebas de trabajo (proof-of-work), esta minería como en Litecoin esta accesible a un mayor número de usuarios, ya que requiere de menos recursos

Lo que lo diferencia con Litecoin es: su expansión y reputación en las redes sociales, tales como Twitter y Reddit, en esta última es la segunda criptomoneda con más seguidores, solo por detrás del Bitcoin, esto ocasiona que su expansión fluya y que forje una comunidad de usuarios, sólida y de ayuda mutua.

Debido al bajo precio de su cotización, las comisiones que se cobran por realizar las transacciones, son incluso menores que en Litecoin y Bitcoin.

El tiempo de transacción es de 60 segundos a diferencia de 2,5 minutos en Litecoin.

El máximo de emisión al comienzo fue 100 mil millones de DOGE con una inflación de 5.256 mil millones cada año. Esto es una clara diferencia con Bitcoin y Litecoin ya que estos últimos siguen una política deflacionaria, mediante la cual emitieron un numero finito de monedas, provocando un mayor acaparamiento por partes delos usuarios ya que el valor real percibido de la moneda aumenta con el tiempo, esto provoca un gasto menor de Bitcoins y una mayor flujo con DOGE.

Su capitalización en el mercado es de 29,298,603 $ con un precio de 0.000284$/DOGE, con un total de 103,189,892,168 DOGE

4.2.5. MaidSafeCoin.

Figura 8. Logo MaidSafecoin.

Este proyecto se llevó a cabo en 2006, desarrollado por David Irvine, junto con un pequeño equipo de trabajo, su objetivo es proporcionar un Internet descentralizado, conseguir seguridad, privacidad y libertad para todo el mundo.

Para ello se crea la red **SAFE Network**, con las siguientes características:

1. Acceder y asegurar la información personal.
   La información del usuario encriptada se encuentra en la red, pero solo podrá ser visualizada con la clave privada del usuario que solo se encuentra en el ordenador personal o incluso en papel y solo con esa clave se puede acceder a la información.

2. Datos que se encriptan con ellos mismos.
   Los datos se envían a la red y se dividen en partes, se encriptan y se distribuyen por toda la red.
3. Existe la Red distribuida que permite el almacenamiento en caché cerca del usuario que la solicita, realizando copias de información que se solicitan frecuentemente.
4. Disponibilidad y redundancia de datos: se realizan copias de cada dato y se distribuye por la red P2P, cambiando la localización de los datos constantemente, haciéndolos prácticamente inmunes a ataques informáticos.

Con esta premisa crean la criptomoneda denominada Safecoin. Es el principal sustento de la red ya que se utiliza para recompensar a los usuarios que desarrollan, y colaboran en el proyecto. El límite estipulado de emisión de esta criptomoneda está en 4.3 mil millones MAID, y está fijado exclusivamente que un 15% del total de Safecoin que se consigue esté destinado a un fondo para los desarrolladores y que éstos continúen con la motivación para seguir con el desarrollo del proyecto. Existen otras formas de

conseguir las criptomonedas, como en el caso de la mayoría, son mediante intercambio o compra y un método nuevo el *farming*[19].

Los *farmers*, que así son denominados los usuarios que se dedican a esta actividad, son similares a los mineros en otro tipo de criptomonedas, pero con diferencias en algunos aspectos como el referente a los *farmers*, que ganan Safecoins proporcionando *Proof of Resource* (Prueba de recursos). Estos *farmers*ejecutan un nodo de red en su ordenador con un software, que maneja peticiones y almacena datos para otros usuarios. Los recursos específicamente son: almacenamiento, potencia de la CPU, tiempo en línea y banda ancha.

La red SAFE es capaz constantemente de medir y verificar estos recursos de manera inmediata. Esto es el *Proof of Resource.* Para ganar Safecoin los *farmers,* al tratarse a la vez de usuarios, deben proporcionar más recursos de los que consumen y cuantos más recursos proporcionan, más obtendrán, pero el sistema funciona también de forma aleatoria ya que la información se almacena aleatoriamente en todos los nodos de la red, cuantos más recursos apliquen los *farmers* más posibilidades tendrán de ganar más Safecoin.

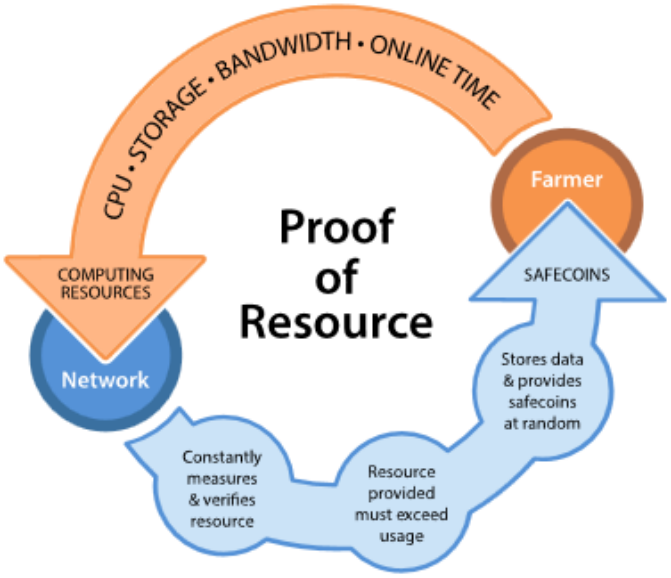


Figura 9. Diagrama del método Proof of Resouce.[20]

[19] *Farming* proviene del inglés, y hace referencia a la actividad de recolección de un determinado producto que se realiza en la agricultura, y se extrapola su significado al mundo de las criptomonedas de realizar la recolección de un determinado producto.

[20] Disponible en:http://maidsafe.net/safecoin.html#proof-of-resource

La capitalización de MaidSafeCoin actualmente es de **27,991,181 $** con un precio por MAID(SafeCoin) de **0.061852 $/MAID** y un volumen total de **452,552,412 MAID.**

Por último me gustaría mencionar el proyecto de criptomoneda Pesetacoin que se inició a principios del año 2014 y que abarca el ámbito nacional.

Figura 10. Logo de Pesetacoin.

Surgió en el contexto de más auge del Bitcoin y las Altcoin y perseguía trasladar la filosofía de estos a España.

Los creadores son los informáticos españoles Ramón Martínez y CryptoMP y ellos mismos la definen en su página web como *"una nueva Cripto-moneda desarrollada a partir de BitCoin y LiteCoin pero enfocada al ámbito español y con minado conjunto."*

Al comienzo del proyecto buscaban un crecimiento paulatino y no causar mucha expectación ni revuelo para evitar los posibles problemas que pudieran surgir como ocurrió con otros proyectos como Dogecoin en los cuales su rápido crecimiento produjo una alta especulación de la moneda y minería instantánea.

El nombre pretende ser un homenaje a la peseta, moneda fiduciaria oficial española que desapareció a finales del siglo pasado con la llegada del euro y entre sus objetivos destacan: el ofrecer a la comunidad el adentrarse y familiarizarse con el entorno Bitcoin en el idioma español, y todos los procesos de intercambio por euros y uso para las compras online en España.

Utiliza el algoritmo Scrypt para el proceso de transacciones a través del método Proof-of-work (prueba de trabajo) como en el caso de Litecoin y Dogecoin y al igual que estas y Bitcoin tienen un número limitado de monedas emitidas para evitar la inflación en este caso es de 166,386,000 PTC siendo un homenaje al valor de referencia fijado en 1998 donde 166,386 pesetas equivalían a 1 euro.

En cuanto a la obtención comparte las mismas características con otras criptomonedas (obtención por donaciones, compra directa, o *faucets*) y permite el

minado conjunto con otras monedas como el Litecoin. El *Wallet* o monedero para almacenar Pesetacoin es "PaperWallet"[21]

A día de hoy el proyecto parece estar en un proceso de parada, aunque no abandonado, ya que no hay nuevas noticias ni comentarios por parte de los desarrolladores, pero la comunidad de usuarios, dentro de la escasa relevancia que tiene, sigue activa.

En el ranking de capitalización de las criptomonedas, se encuentra en el puesto 243 de 682 criptomonedas conocidas dispuestas en este ranking[22].

Su capitalización total es de 19,171 $ con un valor de 0.000166 $/PTC y un volumen total de monedas en circulación de 115,164,649 PTC.

- **DESARROLLO:**

1. **Definición exacta de Bitcoin (Díaz Vico, Sánchez Aragó, 2014):**

El Bitcoin es una bien digital en línea que se basa en la tecnología red entre iguales o P2P "peer -to-peer" para la gestión de transacciones y distribución a diferencia del dinero fiduciario, cuyo valor se deriva a través de la regulación o ley y garantizado por el Estado, los bitcoins no tienen valor intrínseco y el único verdadero valor se basa en la oferta y la demanda, lo que la gente está dispuesta a negociar para ellos.
El bitcoin es descentralizado, no está respaldado por ningún gobierno, ni depende de la confianza de un emisor central.

La capitalización actual de Bitcoin es de 6,464,598,186 $, la mayor entre todas las criptomonedas, con un precio por Bitcoin de 424$/BTC y un total de Bitcoins emitidos de 15,246,550 BTC.[23]

2. **Conceptos generales (Díaz Vico, Sánchez Aragó, 2014) :**

[21] Wallet para Pesetacoin: http://www.pesetacoin.info/paperwallet/
[22] Mercado de capitalizaciones de las principales criptomonedas: https://coinmarketcap.com/
[23] Datos extraídos de Coinmarketcap, consultados el día 22/02/2016. Disponible en: https://coinmarketcap.com/

Para contextualizar y entender los siguientes apartados del estudio y pese a la explicación detallada de los términos más adelante, es necesaria una definición general de los mismos:

Direcciones Bitcoin:

Dirección virtual de un usuario que puede contener Bitcoins u otras criptomonedas y necesaria para pagar y recibir pagos. Un mismo usuario puede tener tantas direcciones como necesite y se identifican mediante una clave pública.
La clave privada asociada sirve para firmar las transacciones y la clave pública sirve para identificar la dirección y validar las firmas.

Monederos o wallets:

Espacio virtual, equivalente a un monedero físico, donde se almacenan y gestionan las direcciones de un usuario y los pagos que se realizan con ellas.

Transacciones:

Una transacción es una transferencia de dinero de una dirección a otra.

Bloques:

Es una estructura que agrupa transacciones. Las transacciones pendientes de confirmar se agrupan en un bloque sobre el que se realiza el denominado proceso de minería.

Cadena de bloques (*blockchain*):

Registro público de las transacciones de Bitcoins u otras criptomonedas, validadas en orden cronológico. Cuando un bloque ha sido confirmado, a través de la minería, éste pasa a formar parte de la cadena.

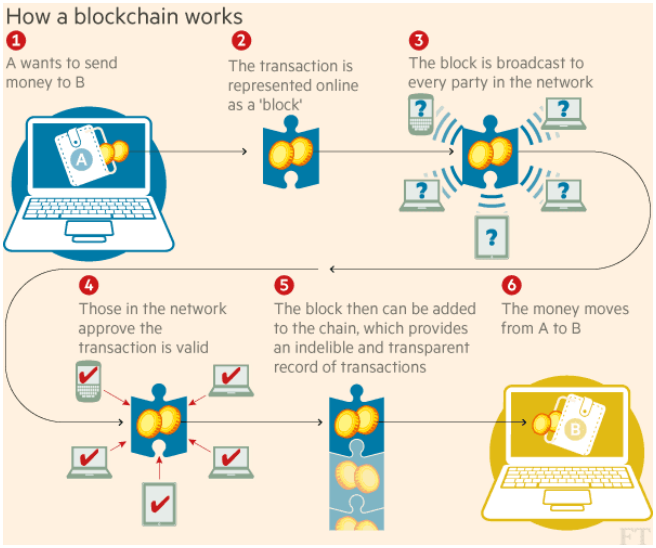


Figura 11. Funcionamiento de la cadena de bloques[24]

Minería:

Proceso de realización de cálculos matemáticos para confirmar transacciones en la red P2P de la criptomoneda. A través de la minería se pueden generar nuevos Bitcoins al mismo tiempo que se confirman transacciones.

3. Cifrado:

El protocolo Bitcoin abarca una serie de procedimientos y procesos que garantiza el funcionamiento de Bitcoin en su totalidad, desde la accesibilidad, la creación de nuevas direcciones, la seguridad etc. A continuación se explica en detalle, el proceso de cifrado:

- Paso 1: utiliza el algoritmo ECDSA *(Elliptic Curve Digital SignatureAlgorithm)* para la creación de claves privadas y públicas. Este algoritmo es una variante del algoritmo DSA[25]al que se le añade la criptografía mediante la criptografía de curva elíptica (ECC). La principal ventaja de utilizar este algoritmo es la posibilidad de crear claves con menor longitud de caracteres, que no ocupen mucho espacio y que se transmitan más rápidamente (Preukschat, 2014).

[24] Disponible en: http://blogs.elconfidencial.com/mercados/valor-anadido/2016-02-05/blockchain-la-tecnologia-que-enloquece-a-la-banca-y-que-tardara-en-llegar_1146555/#lpu65M9nSEbtPVV5

[25] DSA *(Digital SignatureAlgorithm).* Algoritmo de firma digital estándar del Gobierno Federal de los Estados Unidos. Es un algoritmo de firma y no de cifrado. Fuente: https://es.wikipedia.org/wiki/DSA

- Paso 2: el segundo proceso es utilizar 2 funciones hash en las claves. Se utilizan las funciones hash SHA-256[26] y RIPEMD-160[27]. Este último pese a ser un algoritmo casi desconocido, se utiliza para creas los hash más cortos y seguros en la creación de una clave o dirección Bitcoin. SHA-256 se utiliza en combinación con RIPEMD-160, por los riesgos de seguridad del protocolo Bitcoin con las interacciones imprevistas del algoritmo RIPEMD-160 con ECDSA (algoritmo creador del par de claves pública y privada), teóricamente interponiendo el SHA-256 entre el ECDSA y RIPEMD-160 se consigue que no se encuentren colisiones[28] en una dirección pública de Bitcoin. (Preukschat, 2014)

4. Wallets y poseedores (claves públicas y privadas: criptografía asimétrica).

Un wallet o billetera es un archivo necesario para realizar las operaciones de envío y recibo de Bitcoins. Pese a la semántica de billetera no actúa como tal en sentido de que no guarda los Bitcoins en este archivo sino que almacena una serie de claves privadas, y públicas que son únicas y que nos dan el derecho de posesión de los Bitcoins para autorizar o firmar pagos (transferir la posesión de los Bitcoins).

Antes de continuar es oportuno explicar cómo funciona una clave pública y una clave privada, mediante la criptografía asimétrica.

4.1. Criptografía asimétrica:

Se denomina criptografía asimétrica al proceso criptográfico que utiliza dos claves: una pública y otra privada. La clave pública se puede entregar a cualquier persona, funciona como un dirección de correo electrónico o una ID, la clave privada es personal y única y el propietario debe guardarla a buen recaudo para que nadie acceda a ella (Gutiérrez, 2013).

El funcionamiento es el siguiente: un usuario **A** quiere enviar un mensaje a un usuario **B**. El usuario **A** utiliza la clave pública de **B** para cifrar el mensaje una vez cifrado solo la clave privada de **B** podrá descifrarlo.

[26] SHA-256 (Secure Hash Algorithm), conjunto de funciones hash desarrollado por la NSA (Agencia de Seguridad Nacional de los Estados Unidos). Fuente: https://es.wikipedia.org/wiki/Secure_Hash_Algorithm

[27] RIPEMD-160: (acrónimo de *RACE IntegrityPrimitivesEvaluationMessageDigest) Fuente :https://es.wikipedia.org/wiki/RIPEMD-160*

[28] Colisiones en criptografía se produce cuando dos entradas distintas a una función hash producen la misma salida.

Este tipo de criptografía es utilizada en la conocida ***firma electrónica*** pero con otro uso del par de claves por parte del usuario. En este caso el usuario **A** cifra el mensaje con su **clave privada**, envía el mensaje al usuario **B** y este con la clave pública del usuario **A**, puede leer el mensaje y comprobar que la autenticidad es del usuario **A.** Este proceso es similar al utilizado en las **transacciones de Bitcoin**, que se analiza más adelante en el apartado de transacciones.

4.2. Creación y uso de los wallets:

En cuanto al Wallet al contener información de tal relevancia, son numerosos los pasos que se siguen y las recomendaciones por parte de toda la comunidad de Bitcoin para almacenar de forma segura un Wallet. Primero se disponen de distintos métodos para crear un Wallet:

El método más común y el que los usuarios avanzados prefieren, es la descarga de un programa cliente en el ordenador. Este tipo de cliente se debe sincronizar con la red y en general descargar toda la cadena de bloques (transferencias) hasta la fecha en el ordenador del usuario, este proceso es largo, ocupa espacio en el disco duro y puede tardar varias horas o días, y solo se realiza la primera vez que se instala, no cada vez que se accede al Wallet. Hoy en día existen programas cliente como Electrum[29]que no requieren de la descarga completa de la cadena de bloques, sino que accede a un servidor de confianza que contiene toda la cadena de bloques y permite operar desde el momento de su instalación.

El wallet oficial para Bitcoin es **BitcoinCore** se puede descargar para ordenadores con Sistema Operativo Windows, Mac o Linux. Una vez instalado, automáticamente crea el wallet y comienza a descargar el historial de transacciones (cadena de bloques) que es un proc ya se pueden realizar las operaciones de envío y recibo de Bitcoin. Para enviarBitcoin es necesario una conexión a Internet pero para recibirlos no.

Este programa cliente ofrece una clave privada única al usuario para firmar las transacciones y una clave pública. Se recomienda el uso de tantas claves públicas nuevas como transferencias se realicen, pero no es necesario, siempre se puede operar con la misma pareja de claves. No se recomienda la reutilización de una clave pública en nuestro Wallet por problemas de seguridad y privacidad, ya que al utilizar varias claves públicas, la posibilidad de rastreo e identificación son más limitadas.

Las características de los Wallet que se ofrecen hoy en día son similares, y con las siguientes figuras se pretende explicar las funcionalidades, en general, del Wallet cliente más utilizado (BitcoinCore), instalado en un ordenador con sistema Operativo Windows.

[29] Página oficial de Electrum:https://electrum.org/#home

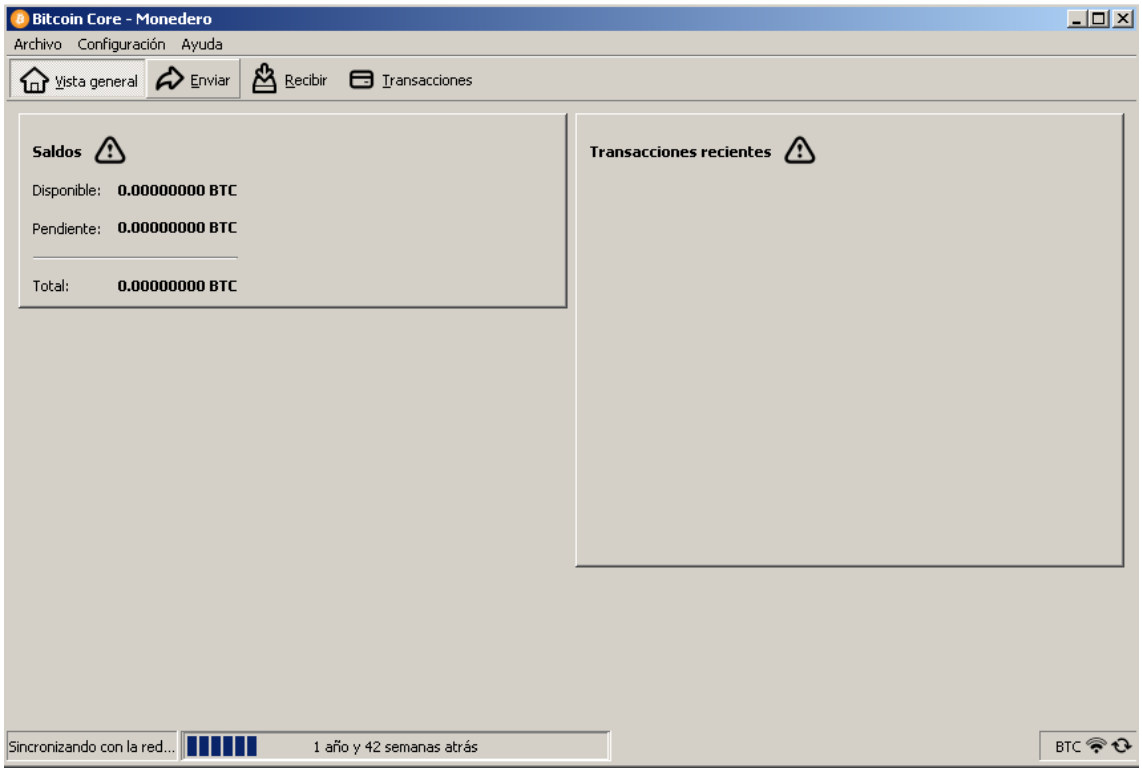


Figura 12. Interfaz general de BitcoinCore.

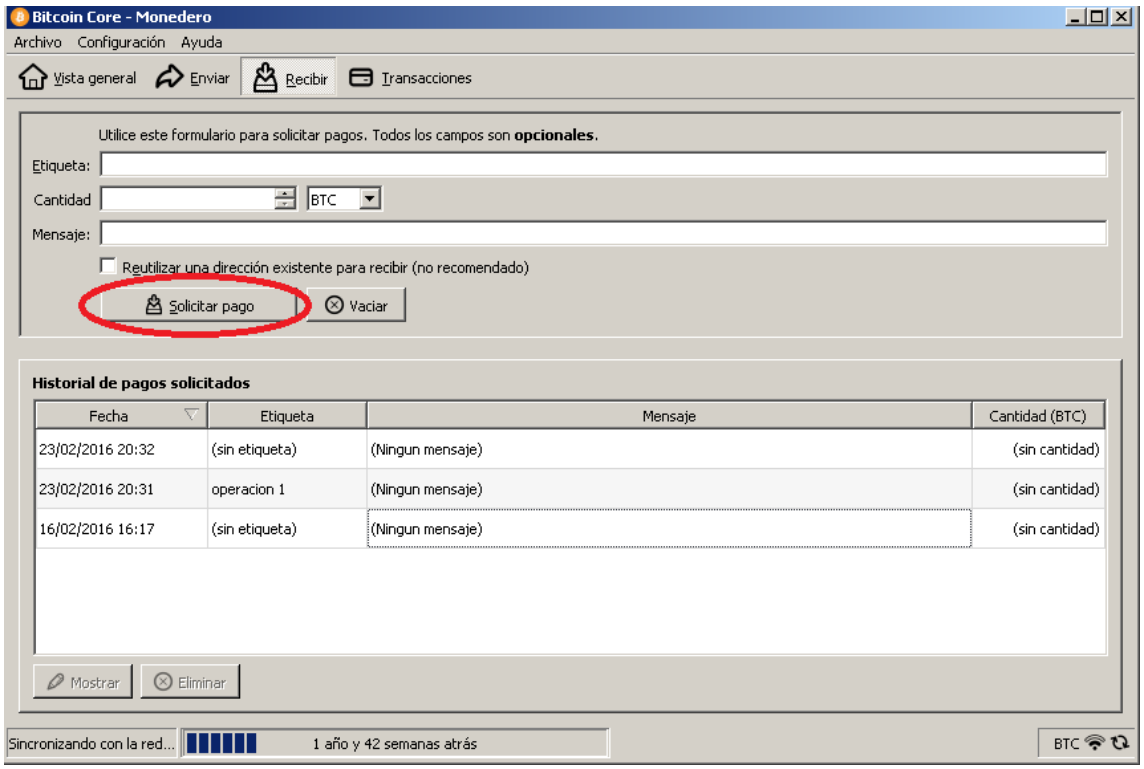


Figura 13. Recibir Bitcoins en BitcoinCore.

Como se muestra en la figura para recibir Bitcoins y facilitar la clave pública se accede a la función **recibir** y a la característica solicitar pago y aparecerá cada vez que se solicite una clave pública nueva por defecto.

En la siguiente figura se muestra la clave pública que se genera con posibilidad de escaneo con código QR*[30]:

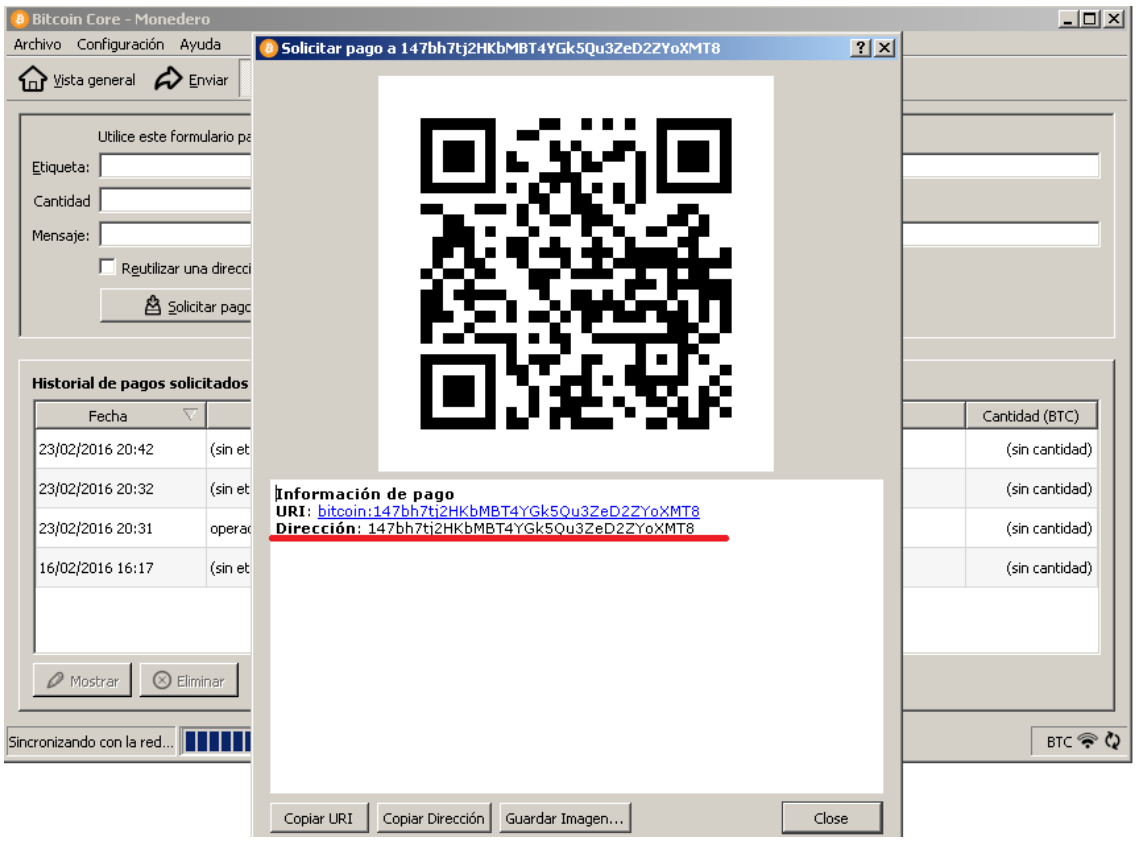


Figura 14. Clave pública en BitcoinCore.

Para el envío de Bitcoin se accede a la función **enviar** y se añade la dirección pública del destinatario en el siguiente campo:

[30] Los códigos QR, (en inglés QR Code) son un tipo de códigos de barras bidimensionales. A diferencia de un código de barras convencional, la información está codificada dentro de un cuadrado, permitiendo almacenar gran cantidad de información alfanumérica. Pueden ser leídos a través de la cámara de un smarthphone que tenga instalado una aplicación para la lectura de estos códigos.

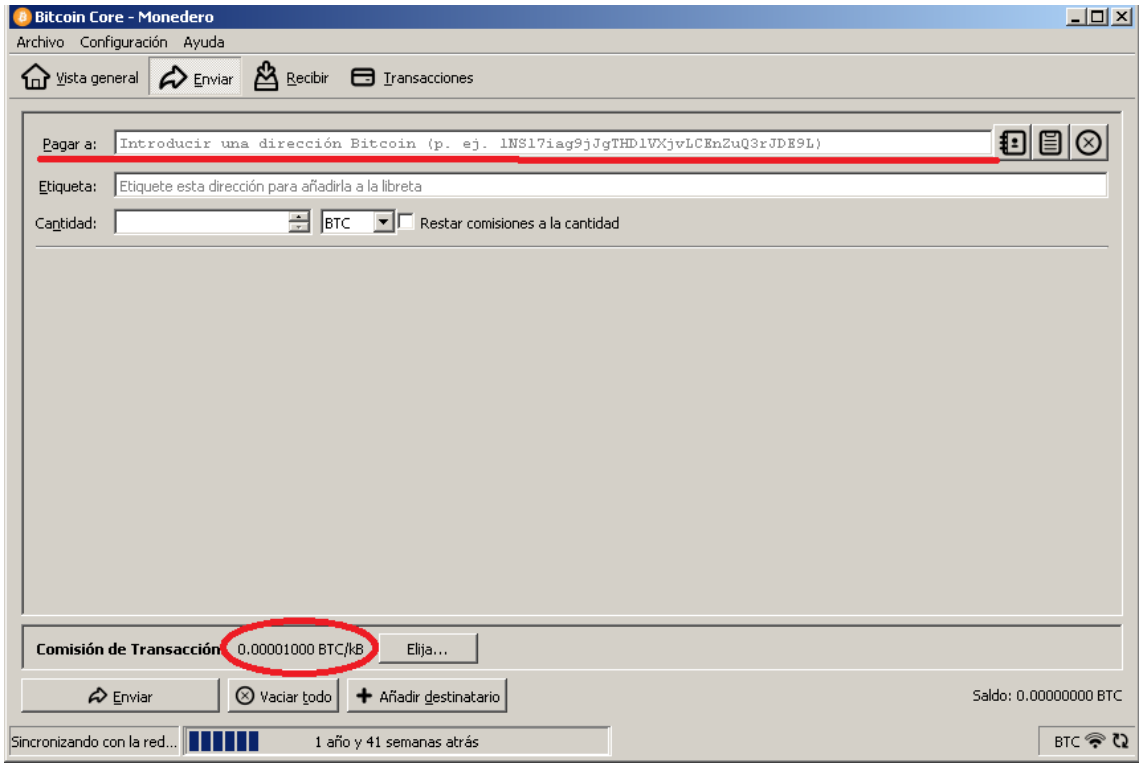


Figura 15. Envío de Bitcoins en BitcoinCore.

Como se aprecia en la figura el envío tiene un pequeño coste de transacción, pero no la recepción de Bitcoins.

Otro método es la creación de un Wallet online, para usuarios inexpertos o que quieran probar con el uso del Bitcoin, es el método más recomendable, ya que no se requiere de la instalación de ningún software en el ordenador y requiere de menos tiempo para empezar a utilizarlos, ya que no se necesita descargar la cadena de bloques, el proceso es sencillo y tan simple como registrarse con una dirección de correo electrónico y una contraseña. Una vez realizado este paso, su uso es igual que el del software cliente instalado en el ordenador. Al igual que con los Wallets que requieren instalar un cliente, existen varias plataformas que ofrecen los Wallets online, el más reconocido es Coinbase[31], pero existen otras plataformas de gran reputación como Blockchain[32]entre otras. La elección de uno u otro por parte del usuario, varía desde la interfaz que ofrece, la seguridad, la reputación y las funcionalidades que cada uno presente.

Comparando los dos tipos de Wallets cabe destacar los aspectos de seguridad que en ambos influyen:

[31] Sitio web oficial de la plataforma Coinbase: https://www.coinbase.com/
[32] Sitio web oficial de la plataforma Blockchain: https://blockchain.info/es/wallet

Por parte de los wallets cliente, la seguridad es buena ya que no exige una conexión constante a Internet para su manejo, los archivos (que contienen las claves públicas y privadas) están descargados de manera local en el ordenador, por lo que para que ocurra un acceso no autorizado, se debe acceder al propio ordenador.

Por otro lado, las plataformas que ofrecen el wallet online al necesitarse de una conexión a Internet en todo momento, son más vulnerables a ataques informáticos.

Pese a esta posible desventaja, en realidad para una seguridad avanzada, lo óptimo sería mezclar ambos servicios, en este caso, crear copias del archivo .wallet y distribuirlos en varios dispositivos físicos que estén bajo el control del usuario como un USB, y aparte importar otra copia al servicio de wallet online de Blockchain, de esta manera si se pierden los archivos en el ordenador o se pierde el USB, siempre se tendrá una copia de respaldo disponible en Blockchain. Por último subir una copia de archivos a la nube, como Dropbox o Google Drive, puede ser una gran idea, pero siempre cifrando los archivos con otra capa superior, con una contraseña fuerte decidida por el usuario, esta funcionalidad la ofrecen programas terceros como 7-Zip[33], de manera que si un atacante accede a este archivo no disponga directamente de la clave privada.

4.3. Monederos de papel.

Otra opción es la creación de "*paperwallets*" o **monederos de papel**. Este método permite almacenar la clave privada sin necesidad de conectarse a la red ni utilizar un ordenador, normalmente la clave privada ocupa unos 51 caracteres, por lo tanto, escribiendo estos caracteres en una hoja de papel, se puede acceder a los Bitcoins en cualquier momento siempre y cuando la aplicación que se utilice para las transacciones de Bitcoin permita importar claves privadas.

Existe la herramienta Bitadress[34], que permite la creación de monederos de papel mediante el lenguaje de programación JavaScript. Desde la página se puede realizar de manera online, o descargar el archivo HTML completo de la página con todas las funcionalidades, desconectarse de Internet y crear los monederos. Una vez creados se puede imprimir, conectando la impresora solo a la red local.

[33] Sitio web oficial de 7-zip:http://www.7-zip.org/
[34] Sitio web oficial de Bitadress: https://www.bitaddress.org/

5. **Minería,** ¿cómo se generan nuevos bitcoins?

Aunque en este estudio, por necesidad, ya se ha mencionado y explicado de forma general el método de la minería, me propongo a analizar este proceso más a fondo y definir las características a las que no se han hecho referencia aún, centrándome en el Bitcoin.

La minería en es el proceso mediante el que los usuarios (denominados mineros) poniendo a disposición de la comunidad en red los distintos recursos de su ordenador, obtienen una cantidad de criptomonedas (Pérez, 2013).

En las distintas criptomonedas que existen, los métodos varían, pero el objetivo es el mismo. P.j.: en Bitcoin se utiliza un método *(Proof-of-work)* y en MaidSafecoin un método *Proof-of-resource*.

Bitcoin utiliza un sistema de prueba de trabajo para la creación de nuevas unidades monetarias y para verificar la validez de las transacciones. En este caso, el sistema de prueba de trabajo permite la transferencia de valor de manera directa entre los participantes de una transacción sin necesidad de depender de ninguna organización central de confianza, ya sea bancos o cualquier otra entidad financiera.

5.1. Método *Proof-of-work* (prueba de trabajo).

Las transacciones se agrupan en bloques. Los mineros de la red P2P de Bitcoin "luchan" para resolver los complejos cálculos matemáticos para procesarlos y ser los primeros en resolver la cadena de bloques (transacciones) y ser recompensados con la criptomoneda. Esta recompensa se obtiene cada 10 minutos, cuando se genera un nuevo bloque con un nuevo Bitcoin sin dueño, que se reparte entre los mineros que han participado en la creación del bloque (OroyFinanzas, 2016).

De tal forma que el mercado va aumentando y la cifra llegará en años a los 21 millones de BTC que es el tope establecido (Satoshi Nakamoto, 2008). Al igual que crece el mercado crece la competencia y son numerosas las empresas que invierten en grandes bienes tecnológicos para soportar la capacidad de procesado, que el método requiere.

5.2. *Pools* (consorcios).

En este contexto surgen las denominadas "*pools"* o consorcios entre usuarios con incapacidad para competir de forma individual con las grandes empresas que compiten en el mercado, de tal forma que prestando los recursos de forma colectiva puedan resolver una cadena de bloques y obtener un beneficio. (CoinDesk, 2014).

Este método ofrece una serie de ventajas y desventajas. La ventaja principal para un usuario que se adentra en el proceso de minado es clara, la posibilidad de obtener una recompensa gracias al consorcio o *pool* que le dará una recompensa si se resuelve la cadena de bloques, en función de los recursos que haya aportado, a más recursos mayor será el porcentaje de Bitcoins que reciba. La desventaja es que, participar en un pool muy repartido, el beneficio para un usuario individual es escaso comparado con los recursos que tiene que apartar al pool, ya que la recompensa es repartida.

Aun así la mejor opción para usuarios nuevos en minería sin muchos recursos, es claramente la unión a un pool. Al igual que para empezar a experimentar con la minería busquen alternativas en las *Altcoins* con menos relevancia y que el proceso de resolución de la cadena de bloques sea más sencillo.

6. **Transacciones**, ¿cómo se evita el uso duplicado de un mismo bitcoin en las transacciones?

Realizar transacciones con Bitcoins es relativamente sencillo, sería como enviar un correo electrónico aunque sin necesidad de registrarse en ninguna plataforma ni de facilitar más información que tu clave pública encriptada (Gaytán, 2015). Para gastar y aceptar bitcoins un usuario se descarga el programa cliente o se utiliza uno online, se asigna una clave pública y una privada para firmar las transacciones y ya se puede operar con ellos, todas las transacciones se publican en un "libro de cuentas" que es la cadena de bloques procesados, que es público en una red descentralizada operado y mantenido por miles de ordenadores en casa, mediante la red P2P (peer-to-peer).
Una vez que la transacción haya sido aprobada por la mayoría de usuarios de bitcoin en la red, la transacción se ha completado y los bitcoins se transfieren de un usuario a otro.
Al usuario que envía los Bitcoins de forma general se le cobra una pequeña comisión, que funciona para beneficiar a los mineros y principalmente como defensa ante usuarios que intenten sobrecargar la red emitiendo pequeñas transacciones constantemente, las cuales tienen que ser todas confirmadas.

Los bitcoins contienen la dirección pública de su dueño. Cuando un usuario *A* transfiere X1 Bitcoins a un usuario *B*, *A* entrega la propiedad agregando la clave pública

de *B* y después firmando con su clave privada. *A* entonces incluye esos bitcoins en una *transacción*, y la difunde a los nodos de la red P2P a los que está conectado. Estos nodos validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla. Para evitar el doble uso de un Bitcoin si A quiere transferir los mismos Bitcoins pero a un usuario C, cuando se detecte la transacción en la red P2P se rechazará automáticamente (Díaz Vico, Sánchez Aragó, 2014).

Las transacciones con bitcoins son: seguras, eficientes, y libres de la presencia de terceros como es un gobierno, el banco, la red de pago, o cámara de comercio. La seguridad se logra a través de una denominada "prueba de cifrado" que permite a las partes en la transacción a tratar directamente unos con otros sin un tercero que autoriza la transacción.

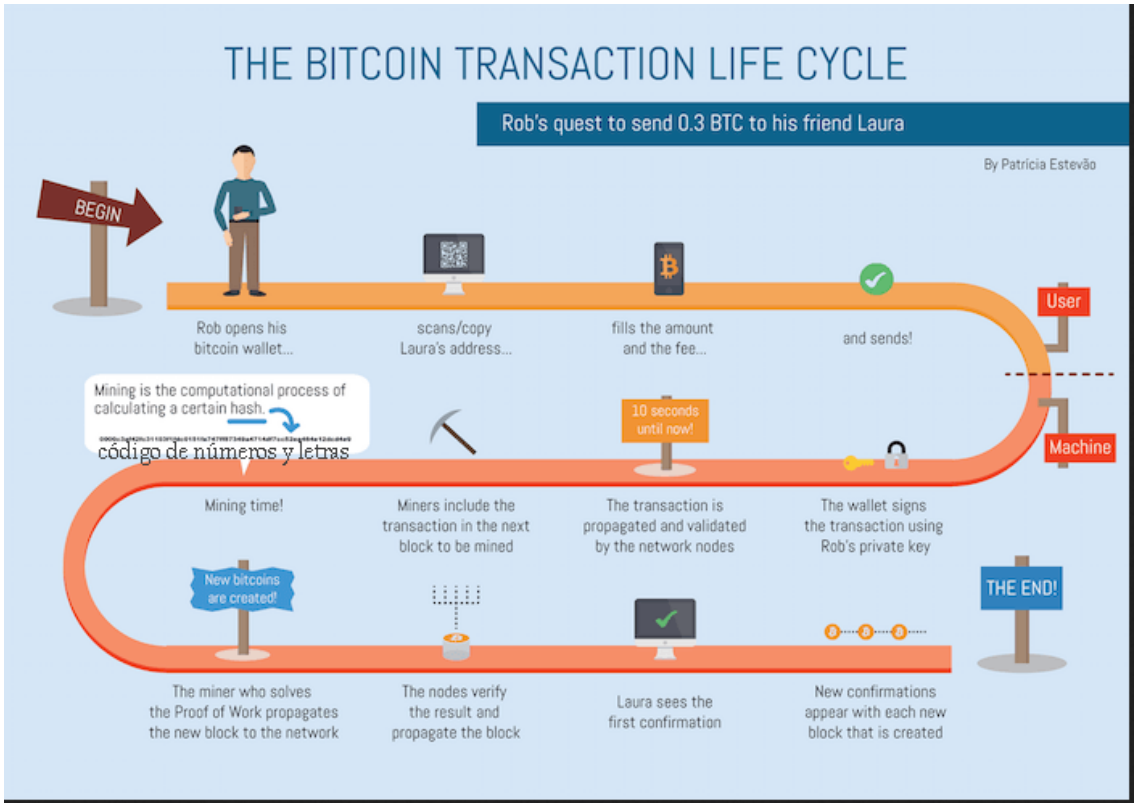


Figura 16. The Bitcoin transaction life cycle.[35]

[35] El ciclo de vida de las transacciones en Bitcoin. Disponible en: https://www.weusecoins.com/en/questions/

7. Trabajo de campo: compra y envío de bitcoins.

Para comprender mejor y experimentar cómo funcionan los intercambios y el manejo en Wallets de una criptomoneda, se ha adquirido una pequeña cantidad de Bitcoins con el fin de analizar el proceso y observar los detalles que conciernen, como la seguridad, y rapidez de las transacciones

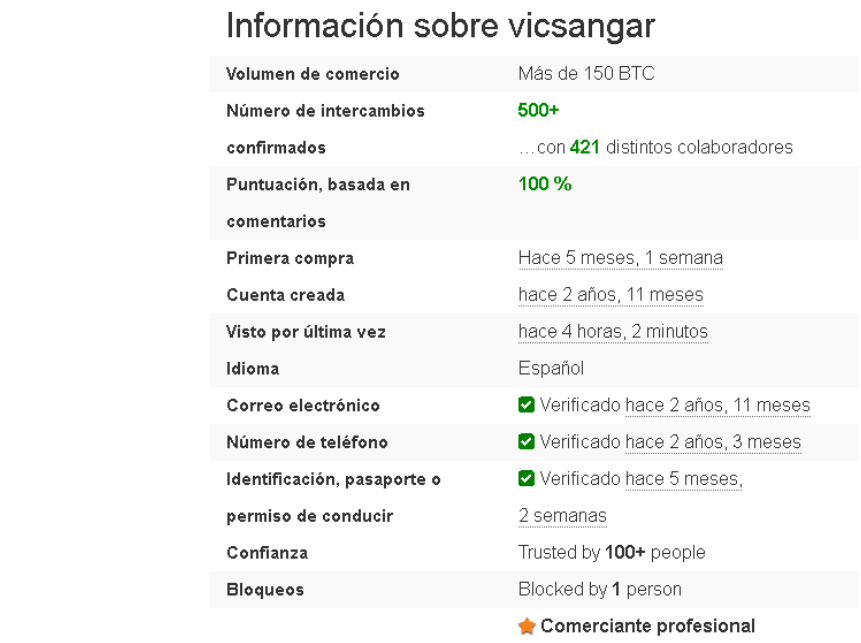
Una de las maneras más sencillas y para usuarios inexpertos que quieran comenzar a familiarizarse en adquirir esta criptomoneda, es realizar esta actividad en un entorno conocido, en el idioma local que mejor se maneje el usuario y que pueda estar en todo momento en contacto con el vendedor.

Una plataforma que ofrece estos servicios es LocalBitcoins[36], una empresa "startup" con sede en Finlandia, la cual ofrece a usuarios de todo el mundo, publicar sus anuncios de compra o venta de Bitcoins, estableciendo ratios de compra y venta y otros usuarios demandan estos servicios y deciden ponerse en contacto con el vendedor/comprador para establecer el método de pago que más les convenga, de manera física, por transferencia bancaria, utilizando servicios como PayPal, etc.

El sistema ofrece entre otras características, la búsqueda de anuncios publicados en una localidad, país, para facilitar el acuerdo entre los usuarios que se involucren. A su vez los usuarios que publican sus ofertas en esta plataforma adquieren un nivel de reputación, según la experiencia, el número de transacciones que ha realizado y los votos de la comunidad.

Para esta prueba decidí adquirir una cantidad de Bitcoins por euros, mediante transferencia bancaria al usuario del siguiente anuncio, basándome en los criterios mencionados anteriormente:

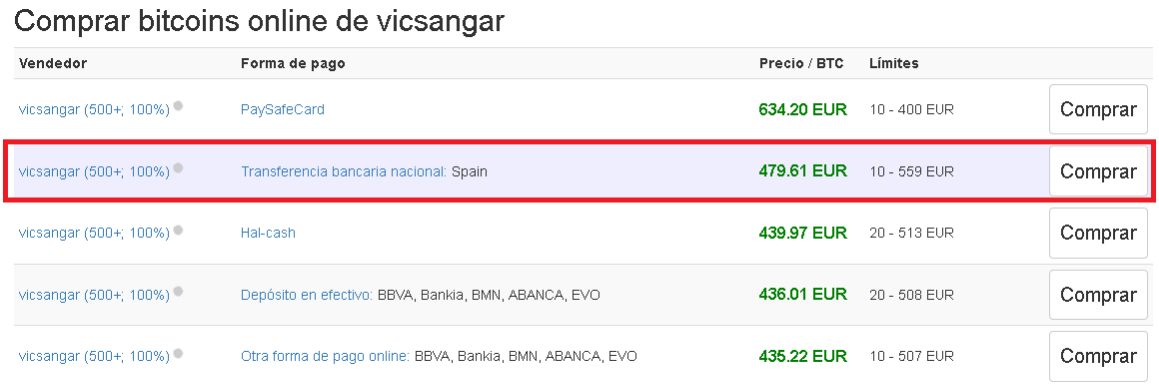
[36] Página de la plataforma LocalBitcoins desde la cual se adquirieron los Bitcoins para la prueba: https://localbitcoins.com/es/



Información sobre vicsangar

Volumen de comercio	Más de 150 BTC
Número de intercambios confirmados	**500+** …con **421** distintos colaboradores
Puntuación, basada en comentarios	**100 %**
Primera compra	Hace 5 meses, 1 semana
Cuenta creada	hace 2 años, 11 meses
Visto por última vez	hace 4 horas, 2 minutos
Idioma	Español
Correo electrónico	✅ Verificado hace 2 años, 11 meses
Número de teléfono	✅ Verificado hace 2 años, 3 meses
Identificación, pasaporte o permiso de conducir	✅ Verificado hace 5 meses, 2 semanas
Confianza	Trusted by **100+** people
Bloqueos	Blocked by **1** person
	★ **Comerciante profesional**

Figura 17. Sistema de reputación de LocalBitcoins.



Comprar bitcoins online de vicsangar

Vendedor	Forma de pago	Precio / BTC	Límites	
vicsangar (500+, 100%)	PaySafeCard	634.20 EUR	10 - 400 EUR	Comprar
vicsangar (500+, 100%)	Transferencia bancaria nacional: Spain	479.61 EUR	10 - 559 EUR	Comprar
vicsangar (500+, 100%)	Hal-cash	439.97 EUR	20 - 513 EUR	Comprar
vicsangar (500+, 100%)	Depósito en efectivo: BBVA, Bankia, BMN, ABANCA, EVO	436.01 EUR	20 - 508 EUR	Comprar
vicsangar (500+, 100%)	Otra forma de pago online: BBVA, Bankia, BMN, ABANCA, EVO	435.22 EUR	10 - 507 EUR	Comprar

Figura 18. Anuncio de Venta de Bitcoins en LocalBitcoins.

Antes de realizar la operación contacté con el usuario para obtener información del proceso y para conocer algún detalle necesario antes de enviar el la transferencia.

El proceso resultó rápido y sencillo, y el usuario respondió a las dudas que se le plantearon de forma casi inmediata. El dinero que se decidió intercambiar fue el mínimo establecido por el vendedor (10 euros). Una vez realizada la transferencia a la cuenta bancaria del usuario, los Bitcoins del vendedor quedan "bloqueados" automáticamente por el sistema de LocalBitcoins y cuando se confirma el pago, el vendedor traslada esos Bitcoins hacia la cuenta de LocalBitcoins del comprador. El proceso tardo un día.

Una vez recibidos los Bitcoins, decidí trasladarlos, debido a que no los iba a utilizar para operar con ellos en LocalBitcoins, al mi wallet online de Blockchain para ver el proceso de traspaso y poder realizar otras transacciones. El proceso es el siguiente y para confirmar el envío es necesaria la contraseña de la cuenta de LocalBitcoins.

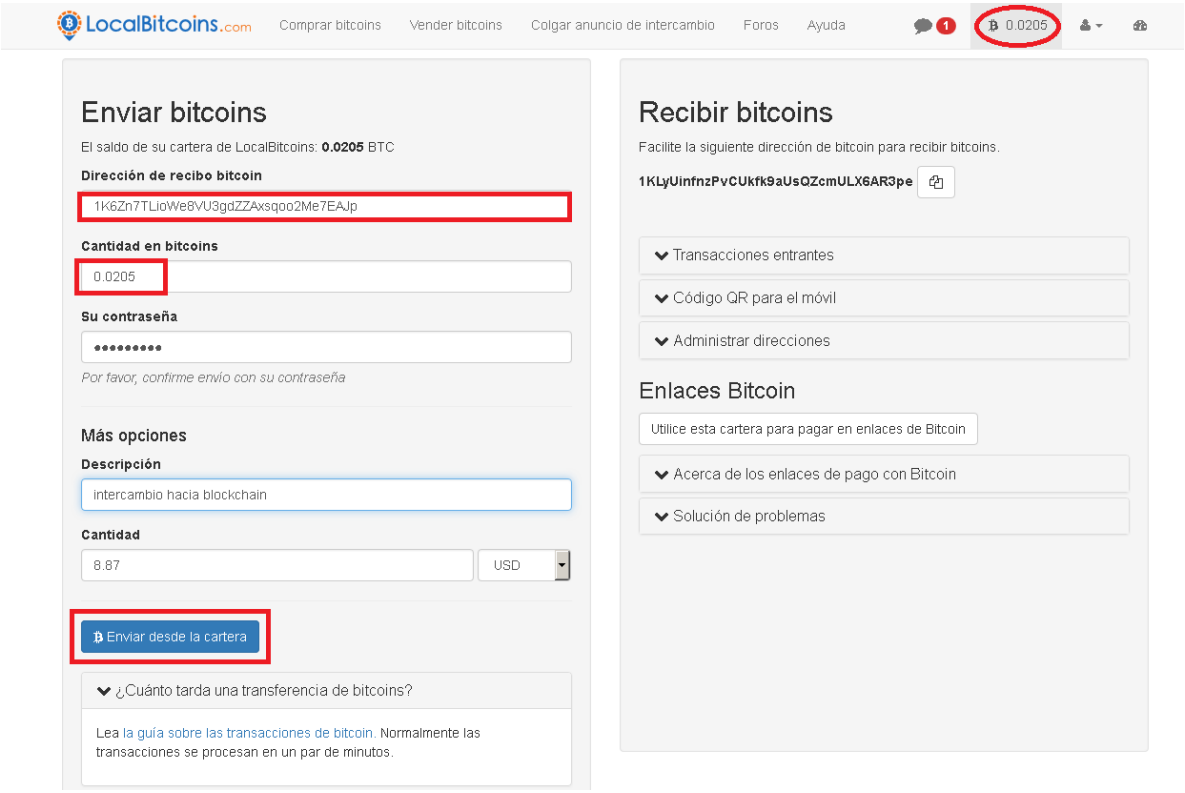


Figura 19. Envío de Bitcoins desde el wallet de LocalBitcoins.

Para realizar este traspaso se añade la dirección pública del wallet al que se desea enviar, en este caso la dirección de mi wallet de Blockchain, en la pestaña *enviar desde la cartera* desde LocalBitcoins.

La transferencia de los bitcoins de una dirección a otra tardó aproximadamente 1 minuto, y está operación no tiene comisión. La primera observación es el valor real de los 10 euros que gasté en bitcoins en LocalBitcoins, este es mucho menor al cambio a dólares y el valor real de los 10 euros equivale a 8.85 $ de bitcoins, según el valor de mercado que establece Blockchain. Esto es debido a que el vendedor de bitcoins debe declarar el IVA, como se explica en el apartado de normativa y facturación, y se le añade el porcentaje al precio que paga el cliente, recibiendo menos bitcoins.

Con los bitcoins en el wallet de Blockchain se decide realizar un envío a otra dirección pública de Bitcoin para comprobar también el funcionamiento de este proceso en Blockchain:

Figura 20. Balance en Blockchain.[37]

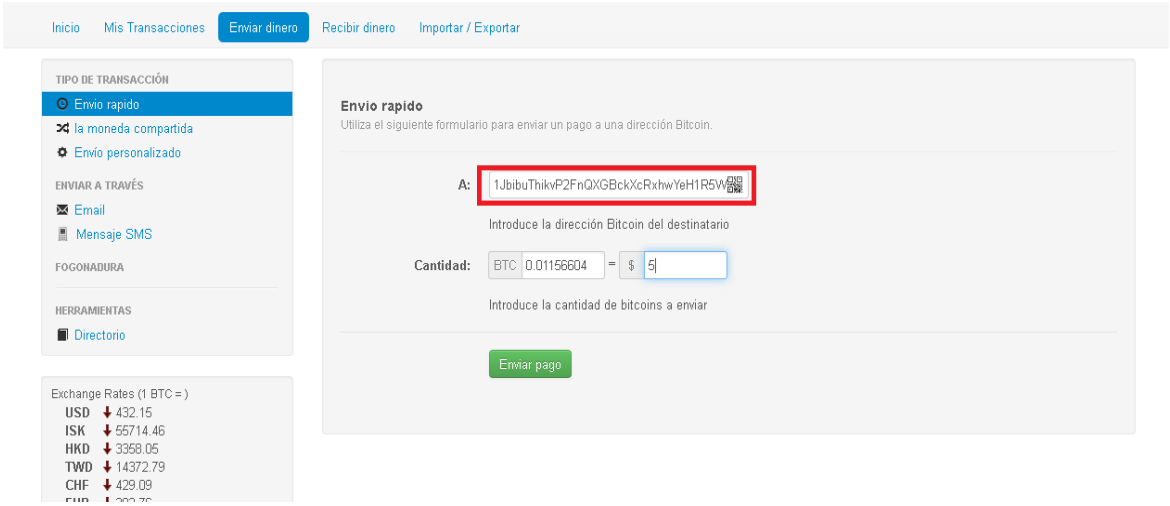


Figura 21. Envío desde Blockchain[38]

Una vez enviados los Bitcoins a la otra dirección comprobamos que han llegado correctamente:

[37] Se observa que la dirección Bitcoin que aparece en la imagen es la que hemos introducido en LocalBitcoins para el traspaso de Bitcoins de una cuenta a otra y que el total de Bitcoins se sitúa ahora en el wallet de Blockchain.

[38] Se realiza el envío a otra persona, conociendo su clave pública.

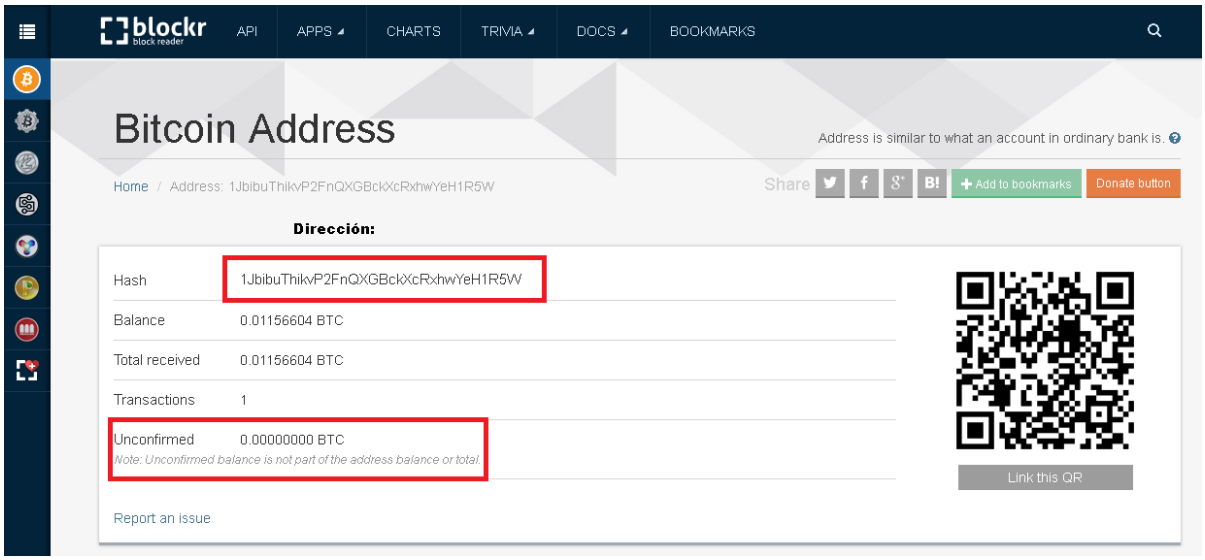


Figura 22. Comprobación del envío de Bitcoins a la otra dirección[39]

8. Uso del bitcoin en el día a día.

Para el comercio con Bitcoins es siempre necesario el uso de wallets que son ejecutados principalmente por ordenador, pero aparece un problema cuando una persona se encuentra físicamente en una tienda y quiere adquirir productos de esa tienda porque acepta Bitcoins, ¿Cómo se puede trasladar el Wallet para realizar estos pagos de manera "física"? En cuanto surgió esta problemática, surgieron los proyectos de carteras físicas y las aplicaciones para Smartphone que numerosas empresas del sector tecnológico y del Bitcoin ya ofrecen, y son versiones para Android, IOS, etc. de los Wallets cliente o de las versiones online. Debido a la inmersión tecnológica de nuestra sociedad interconectada, esto produce un gran paso en el ámbito del Bitcoin, permitiendo la disponibilidad del Wallet por parte del usuario en todo momento.

Algunos de los proyectos más famosos de carteras físicas de Bitcoins son los creados por la empresa TREZOR, las principales ventajas que ofrecen son la seguridad y la portabilidad.

Debido a que el almacenamiento de las claves es físico, es potencialmente más seguro, y ofrecen la posibilidad de firmar transacciones fuera de línea e iniciar sesión de forma segura a sitios web.

[39] La plataforma Block reader nos permite entre, otras características, ver el estado de la transacción que hemos realizado. Disponible en: http://blockr.io/

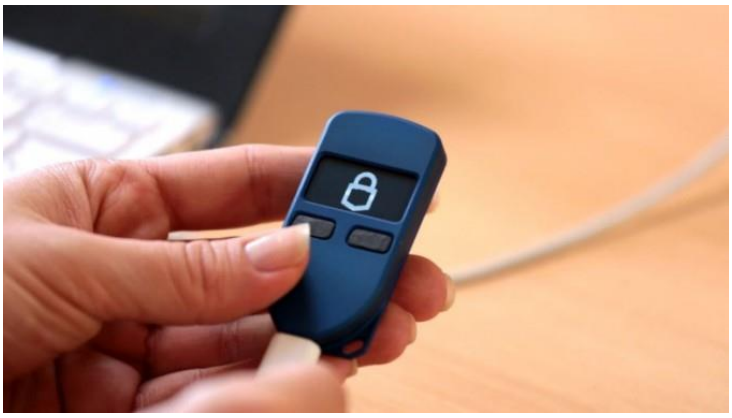


Figura 23. Cartera física de Bitcoins TREZOR.[40]

Hoy en día el uso de esta cartera física de Bitcoin no está muy acogido debido al alto precio de venta (100$), seguramente incentivado por el coste de producción y desarrollo de este tipo de producto (Hajdarbegovic, 2014).

El uso del Bitcoin en el día a día está más enfocado al medio online que en su uso en tiendas físicas o mercados, aunque son numerosos las tiendas físicas que cada vez más permiten pagos con Bitcoins, por ejemplo en tiendas de Nueva York, Londres y Madrid donde varios establecimientos de la calle Serrano permiten el pago con Bitcoins.

En Barcelona se está llevando a cabo un proyecto desde el 2014, similar al de Madrid, en el que voluntarios usuarios de esta moneda, pretenden que numerosos comercios adopten esta nueva forma de pago.

El lugar elegido es el districto de Ciutat Vella, lugar céntrico de Barcelona, con visitas turísticas, donde la ejecución de este proyecto se pueda llevar a cabo de la mejor manera posible. Ya existen dos cajeros en Barcelona y L'Hospitalet que permiten la compra y venta de Bitcoins, algo muy útil por ejemplo para usuarios extranjeros de Bitcoins que vienen a nuestro país y pueden intercambiar esta moneda virtual por la moneda local, ahorrándose hasta un 90% de las comisiones tradicionales. (Martínez, 2014)

En Madrid ya se instaló el primer cajero Bitcoin de España a comienzos del año 2014, y actualmente ya hay distribuidos cajeros Bitcoin por otras ciudades españolas como Guadalajara, Castellón y Vitoria.[41]

A continuación Mapa de comercios que aceptan Bitcoins en España:

[40] Imagen disponible en: http://www.coindesk.com/trezor-hardware-wallet-ship-january/
[41] Plataforma para buscar cajeros automáticos donde operar con Bitcoins: https://www.territoriobitcoin.com/category/bitcoin/cajeros-automaticos/

Figura 24. Mapa de comercios que aceptan Bitcoins en España.[42]

6 años después de su aparición, el mundo del Bitcoin y las criptomonedas es más reconocido, su tecnología, el uso en el día a día y su evolución, llama la atención a las grandes empresas como BBVA Ventures, el grupo de capital riesgo que invierte en *"startups"* del grupo BBVA, que ha decidido invertir en Coinbase, la plataforma líder para realizar transacciones con la divisa virtual Bitcoin, sin duda supone un gran paso en el acercamiento de este ámbito a la institución (Gómez,2015).

Por su parte el Banco Santander realizó un estudio sobre las ventajas que ofrece la tecnología de bloques (*blockchain*) que ofrecían proyectos como el de Bitcoin, denominado Informe FinTech 2.0[43], pone de manifiesto el ahorro de costes (cerca de 15 y 20 mil millones de dólares) que supondría la implementación de esta tecnología en la infraestructura de los bancos para el año 2022, erradicando los organismos que funcionan como autoridades centrales, que hacen más costoso, en tiempo y dinero, el proceso. (Novoa, 2015)

[42] Disponible en línea en el informe del Instituo Nacional de Ciberseguridad: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf [Consultado el 15 de septiembre de 2015]

[43] Acceso completo al Informe FinTech 2.0 del banco Santander : http://santanderinnoventures.com/fintech2/

Con su grupo de inversiones de capital riesgo InnoVentures, el Banco Santander se ha introducido en el mercado de la criptomoneda, invirtiendo 4 millones de dólares en Ripple y pasando a formar parte de su junta directiva. (Novoa, 2015)

Esto indica, que se toma más enserio el entorno Bitcoin, cada vez son más las empresas relevantes que quieren participar de esta tecnología innovadora del Bitcoin que ha traído cambios en la forma que se realizan los pagos y transacciones a nivel mundial y que tiene la oportunidad de evolucionar y seguir cambiando este sistema en un futuro, con el acercamiento a la institución por medio de estas empresas.

8.1. Los Exchanges (intercambiadores).

Con la creación del bitcoin, surgen centros de intercambio de Bitcoin con otras divisas mundialmente aceptadas como el Dólar y el Euro. Estos centros son conocidos como Exchangers (intercambiadores). Son mercados financieros que permiten **bajo el libre juego de oferta y demanda** darle un valor económico a la criptomoneda.

Son una parte integrada del ecosistema en sí de las monedas virtuales, y del sistema Bitcoin. Funcionan como intermediarios entre compradores y vendedores. Los usuarios pueden establecer un precio fijo al que vender/comprar Bitcoins. Estos intercambiadores enlazaran a los compradores y vendedores cuando las condiciones de ambos coincidan. Por ejemplo:

Un vendedor deposita una cantidad X de BTC con la dirección del Exchange (intercambiador), entonces puede usar su balance positivo en Bitcoins en el intercambiador para venderlos por Dólares u otras monedas. De igual forma ocurre con el comprador, deposita X dólares con el intercambiador y con esa balance positivo compra Bitcoins de los vendedores, ambos comprador/vendedor con los precios mínimos y máximos que hayan establecido.

8.2. Casos de quiebra y fraude.

Hasta comienzos de marzo de 2016 ya son dos grandes Exchanges los que se han declarado en banca rota y han sufrido robos o ataques cibernéticos. El más grave y que suscitó la mayor polémica en cuanto a la seguridad del Bitcoin fue el principal Exchange hasta el año 2013 fue Mt.Gox, que por entonces manejaba el 70% de las transacciones de Bitcoins. A comienzos del año 2014 se declaró en bancarrota, dejando de ofrecer sus servicios de intercambios, y permitiendo así al tribunal buscar un comprador. A continuación comenzó el proceso de liquidación, anunciando que alrededor de 850,000 Bitcoins (cantidad equivalente a 450 millones de dólares por entonces) que pertenecían a clientes y a la propia compañía, habían desaparecido y que posiblemente fueron robados. Se consiguieron recuperar finalmente 200,000, y

alegaban que las razones por las que había desaparecido tal cantidad de Bitcoins fueron un cúmulo de la mala gestión, fraude y robo. (Fargo, 2015).

Tras la caída de este monopolio que tenía la empresa Mt.Gox nuevos Exchanges cobraron fuerza y se ganaron una buena reputación entre la comunidad que se mantiene hoy en día como por ejemplo es el caso de Coinbase.

Por el contrario Cryptsy, otro Exchange no se mantuvo mucho más y se encuentra actualmente a punto de la banca rota, la plataforma permanece congelada, no permite la retirada de fondos ni realizar ninguna operación. Sus creadores están en búsqueda de un comprador que pueda hacer frente a los aproximadamente 10.000 Bitcoins (unos 4 millones de dólares) que tiene en deuda de las pérdidas ocasionadas por el robo de más de 9 millones de dólares en Bitcoins y Litecoins en el mes de julio de 2014, del que apenas se informó y del que aparentemente consiguieron recuperarse por los ingresos que generaba la empresa (OroyFinanzas, 2016).

Según citan sus creadores fue a finales de 2015 cuando empezaron los problemas más graves, tras la publicación de una investigación (según ellos llena de acusaciones falsas) en la cual participaron numerosas agencias federales y de seguridad como la Securities and Exchange Commission y la *Criminal Investigation Division of the Internal Revenue Service* entre otras, en la que se destapan, entre otros, los siguientes hechos: la relación entre miembros de Cryptsy con operaciones fraudulentas de la empresa GAW miners[44], la manipulación de mercado, la venta de valores sin licencia y el lavado de dinero (Coin Fire, 2015).

En este contexto fueron muchas las voces que proclamaban la falta de seguridad que rodea este entorno, al no ser respaldados por gobiernos ni entidades centrales y de los peligros que podía ocasionar el uso de Bitcoins, aumentando así la "mala fama" del Bitcoin que ya le caracterizaba en ciertos ámbitos.

• CONCLUSIONES:

En este estudio, se ha presentado un análisis de las características del Bitcoin y el entorno que rodea a las criptomonedas.

En cuanto a la legalidad el Bitcoin y el entorno que le rodea sigue suscitando ciertas dudas y son bastantes las instituciones y paises que aún a día de hoy se muestran

[44] Gaw miners empresa relacionada con la minería de Bitcoin y Altcoins, que se demostró que realizó una estafa mediante un proyecto de caridad relacionado con la memoria del 11-S. Fuente: http://www.coinbuzz.com/2015/04/17/breaking-gaw-miners-ceo-admits-to-charity-fraud-scandal-continues/

precavidos y limitan o incluso prohíben en algunos casos su uso como el de cualquier otro bien.

En lo referente al análisis de la capitalización mencionar que se trata de un mercado volátil, el precio del Bitcoin y las criptomonedas fluctúa constantemente en función de la confianza de los usuarios ya que es frecuente encontrar diferencias en el ranking de posicionamiento de las Altcoins en cuestión de días o incluso horas. En esta confianza influyen entre otros aspectos, los cambios constantes y a la evolución de los proyectos derivados del mismo prototipo que Bitcoin, que implementan nuevas funciones, adquieren nuevas tecnologías, nuevos inversores y generan unas expectativas y un riesgo a tener en cuenta por parte del invensor o la comunidad de usuarios.

Mediante la prueba se ha observado que la teoría es aplicada a la práctica, las transacciones se han realizado de forma rápida, como se ha decidió utilizar un servicio de wallet online, la creación del mismo ha llevado minutos, han sido completamente anónimas, solo se necesita conocer la clave pública a la que enviar y facilitar tu clave pública para recibir.

En el caso del pago con euros en el exchange LocalBitcoins, se aprecia que el precio de compra fue alto, se gastaron 10 euros para intercambiarlos por 0.02050000BTC y esta misma cantidad cuando la trasladé a Blockchain, como se aprecia en las imágenes, estaba valorada en 8.85 $. Esto se debe al que en LocalBitcoin cada vendedor establece el precio de venta que desee y debe declarar el iva, la ventaja fue la localización, el idioma para contactar con el vendedor y el método de pago.

La transacción llegó a tardar hasta 1 día debido a que el pago de 10 euros se realizó entre dos entidades bancarias distintas y hasta que no se confirma el pago, por seguridad, el vendedor de Bitcoins no libera la cantidad correspondiente.

El mismo proceso de prueba se han “testeado” los distintos métodos. Se han transferido 10 euros de una cuenta bancaria a otra, y el proceso ha tardado 1 día, cuando se realizó el intercambio del equivalente a 5 dólares (unos 0.01166604 Bitcoins) entre mi dirección de Blockchain y otra, el proceso llevo 12 minutos, por lo que desde mi propia experiencia se observa que la velocidad de las transacciones es una de las primeras ventajas que se aprecian. Como desventaja mencionar que las transacciones cargaron una pequeña comisión de 0.0001 BTC, que para transacciones con cantidades pequeñas, es bastante.

Se concluye mediante el estudio, que el Bitcoin surgió en el mejor contexto posible, en el que la web 2.0 descentralizaba la manera de difundir la información a través de Internet, en un contexto en el que los usuarios forman parte del proceso de creación, difusión y consumo de la información, y funcionan de manera independiente, en el que las redes sociales crecían y se convertían en el motor de las tendencias a nivel global.

Pero el sector bancario y monetario se estancaba, no evolucionaba en absoluto, las transacciones a nivel mundial seguían tardando días o semanas, debido al complejo sistema centralizado en el que intervienen distintas autoridades centrales, aspecto que no tiene ningún sentido en un mundo globalizado y plenamente inmerso en Internet y con las tecnologías móviles cada vez más adaptadas al mundo cotidiano.

Es por lo que se entiende que surja un proyecto como el Bitcoin que va mucho más allá de ser un simple bien digital. El cual renueva y facilita la forma en la que se realizan intercambios de capital a nivel local, nacional e internacional, de una manera anónima: como en un principio surgió Internet, segura: mediante la criptografía y reduciendo costes de tiempo y dinero: sin que intervengan numerosas autoridades que ralentizan y encarecen el proceso, que no son necesarias para que, estableciendo el símil, dos usuarios se envíen un correo electrónico.

En cuanto a la relación que se establece entre Bitcoin y *deep web* o Internet oculto mencionar que pese a todas estas controversias la *deep web* en general, es un conjunto de información que puede ser utilizada por investigadores y curiosos sin ningún tipo de fin delictivo, aspecto que la gente no entiende muy bien debido a todos los mitos y leyendas que surgen de ella.

Por último recalcar que pese a la controversia que suscita su uso, legalidad, seguridad y los casos de robos o quiebras de entidad que manejaban bitcoins y criptomonedas, pone de manifiesto la duda de que si el bitcoin y las criptomonedas serán el dinero del futuro, pero lo que sí se concluye es que su tecnología y las innovaciones del proyecto, con la inversión que se está realizando hoy en día por parte de grandes empresas de todo el mundo, pueden implementarse en el sistema monetario-bancario conocido y promover una evolución.

- **BIBLIOGRAFÍA:**

BERNARDO, Ángela. Bitcoin es legal: ¿verdadero o falso? *Hipertextual* [en línea]. Marzo del 2013. [Consultado el 1 de mayo de 2015]. Disponible en: http://hipertextual.com/2013/03/bitcoin-es-legal

JANSEN, M.A.. Bitcoin - The Political 'Virtual' of an Intangible Material Currency. *Utrecht University* [en línea]. 2012. [Consultado el 15 de mayo de 2015]. Disponible en: http://dspace.library.uu.nl/handle/1874/254739

PÉREZ RODRÍGUEZ, Victor. La Justicia de Japón desacredita el Bitcoin. *Computerhoy.com* [en línea]. Agosto del 2015. [Consultado el5 de septiembre de 2015]. Disponible en:http://computerhoy.com/noticias/life/justicia-japon-desacredita-bitcoin-32567.

GUTIÉRREZ, Pedro. Tipos de criptografía: simétrica, asimétrica e híbrida. *Genbeta:dev* [en línea]. Enero del 2013. [Consultado el 3 de diciembre de 2015]. Disponible en: http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

CAFFYN, Grace. Bitcoin on the Dark Web. *CoinDesk* [en línea]. Septiembre del 2015. [Consultado el 3 de octubre de 2015] Disponible en: http://www.coindesk.com/bitcoin-on-the-dark-web-the-facts/

HAJDARBEGOVIC, Nermin. Review: Bitcoin "Vault" Trezor Lives up to its Name. *CoinDesk* [en línea]. Octubre del 2014. [Consultado el 15 de octubre de 2015]. Disponible en: http://www.coindesk.com/review-bitcoin-vault-trezor-lives-name/

SATOSHI, Nakamoto. Bitcoin: un sistema de dinero en efectivo electrónico *peer-to-peer*. *Bitcoin Organization* [en línea]. Noviembre del 2008. [Consultado el 2 de abril de 2015]. Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

PAÚL GUTIÉRREZ, Jesús. Patrón Oro. *Expansión* [en línea]. [Consultado el día 3 de febrero de 2016]. Disponible en: http://www.expansion.com/diccionario-economico/patron-oro.html

PÉREZ, David. Guía rápida para "minar" Bitcoins desde el ordenador de tu casa. *El Confidencial* [en línea]. Abril de 2013. [Consultado el 7 de octubre de 2015]. Disponible en: http://www.elconfidencial.com/tecnologia/2013-04-13/guia-rapida-para-minar-bitcoins-desde-el-ordenador-de-tu-casa_767386/

GAYTÁN, Cesar. Guía para principiantes en Bitcoin. *BitAPeso* [en línea]. Agosto del 2015. [Consultado el 10 de octubre de 2015]. Disponible en: http://bitapeso.com/guia-para-principiantes-en-bitcoin/

NOVOA, Jaime. El Banco Santander se acerca a Bitcoin e invierte 4 millones en Ripple. *Marketing4ecommerce* [en línea]. Octubre del 2015. [Consultado el 7 de noviembre de 2015]. Disponible en: http://marketing4ecommerce.net/el-banco-santander-se-acerca-a-bitcoin-e-invierte-4-millones-en-ripple/

GÓMEZ, Iván. ¿Quieres saber de Bitcoin? BBVA te explica. *Criptonoticias* [en línea]. Agosto de 2015. [Consultado el 16 de diciembre de 2015]. Disponible en: http://criptonoticias.com/quieres-saber-de-bitcoin-bbva-te-explica/

BECERRA GUITIERREZ, Juan Armando. Mitos y realidades de la Internet profunda | *Revista.Seguridad* [en línea]. Marzo de 2014. [Consultado el 1 de marzo de 2016]. Disponible en: http://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-internet-profunda

DÍAZ VICO, Jesús; SÁNCHEZ ARAGÓ, Antonio. Bitcoin: una moneda criptográfica. *INTECO (Instituto Nacional de Tecnologías de la Comunicación).* [en línea]. Febrero de 2014. [Consultado el 15 de septiembre de 2015]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf

Bitcoin.org. ¿Cómo funciona Bitcoin? *Bitcoin*. [en línea]. [Consulta: 2 mayo 2015]. Disponible en: https://bitcoin.org/es/como-funciona.

TOBAR, Eugenia. La situación legal del Bitcoin en un mapa interactivo. *Maestros del Web* [en línea]. Enero de 2014. [Consultado el 5 de mayo de 2015]. Disponible en: http://www.maestrosdelweb.com/bitcoin-mapa-interactivo/

The Law Library of Congress. Regulation of Bitcoin in Selected Jurisdictions [en línea]. Enero de 2014. [Consultado el 7 de septiembre de 2015].Disponible en: http://cdn1.sbnation.com/assets/3952017/2014-010233_Law_Library_of_Congress_Bitcoin_jurisdictional_survey.pdf

TECAYEHUATL, Eric. ¿Qué es exactamente el Bitcoin? *Gizmodo en Español* [en línea]. Octubre del 2013. [Consultado el 15 de mayo de 2015]. Disponible en: http://es.gizmodo.com/a-todo-esto-que-es-el-bitcoin-472097486

FERNÁNDEZ BURGUEÑO, Pablo. 12 cosas que deberías saber antes de usar bitcoins. *Abanlex* [en línea]. Noviembre de 2013. [Consultado el 25 de abril de 2015]. Disponible en: https://www.abanlex.com/2013/11/12-cosas-que-deberias-saber-antes-de-usar-bitcoins/

ELECONOMISTA.ES. El auge de Bitcoin: ¿una amenaza real para el euro y el dólar? *elEconomista.es* [en línea]. Marzo del 2013. [Consultado el 2 de abril de 2015]. Disponible en: http://www.eleconomista.es/divisas/noticias/4698787/03/13/El-auge-de-Bitcoin-Una-amenaza-real-para-el-euro-y-el-dolar.html

COIN FIRE. Federal Investigation of Cryptsy Underway. *99 Bitcoins*.[en línea]. Octubre del 2015. [Consultado el 5 de noviembre de 2015]. Disponible en: https://99bitcoins.com/federal-investigations-of-cryptsy-underway/

PREUKSCHAT, Alex. ¿Cómo se crea una dirección o clave pública en Bitcoin? *OroyFinanzas: diario digital del dinero* [en línea]. Enero del 2014. [Consultado el 20 de mayo de 2015] Disponible en: https://www.oroyfinanzas.com/2014/01/como-crea-direccion-clave-publica-bitcoin/

OroyFinanzas. ¿Estás perdido en el debate de los bloques Bitcoin? Todas las claves sin importar tu nivel de conocimiento. *OroyFinanzas: diario digital del dinero* [en línea]. Enero del 2016. [Consultado el 7 de febrero de 2016]. Disponible en: https://www.oroyfinanzas.com/2016/01/perdido-debate-bloques-bitcoin-todas-claves-sin-importar-nivel-conocimiento/

OroyFinanzas. Cryptsy, el nuevo Mt.Gox del ecosistema Bitcoin, anuncia su quiebra inminente. *OroyFinanzas: diario digital del dinero* [en línea]. Enero del 2016. [Consultado el 20 de enero de 2016]. Disponible en: https://www.oroyfinanzas.com/2016/01/cryptsy-nuevo-mt-gox-ecosistema-bitcoin-anuncia-quiebra-inminente/

MARTÍNEZ, ISABEL. Barcelona proyecta su primera calle comercial donde pagar con bitcoins. *La Vanguardia* [en línea]. Noviembre de 2014. [Consultado el 5 de septiembre de 2015]. Disponible en: http://www.lavanguardia.com/local/barcelona/20141126/54420228843/barcelona-calle-pagar-bitcoins.html

FARGO, Scott. The Mt. Gox Post-Bankruptcy Claims: A Detailed Guide. *Blockchain Agenda* [en línea]. Mayo de 2015. [Consultado el 7 de septiembre de 2015]. Disponible en: http://insidebitcoins.com/news/the-mt-gox-post-bankruptcy-claims-a-detailed-guide/32357

MIRANDA, Luis. Tailandia es el primer país en prohibir el uso de Bitcoin. *FayerWayer* [en línea]. Julio del 2013. [Consultado el 3 de octubre de 2015]. Disponible en: https://www.fayerwayer.com/2013/07/tailandia-es-el-primer-pais-en-prohibir-el-uso-de-bitcoin/

KRISTOUFEK, Ladislav. BitCoin meets Google Trends and Wikipedia*:* Quantiying the relationship between phenomena of the Internet era. *Scientific Reports 3, 5-5* [en línea]. Diciembre del 2013. [Consultado el 10 de octubre de 2015]. Disponible en: http://www.nature.com/articles/srep03415

KLEIMAN, Jared A. Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare. *American University Washington College of Law 4, no.1, 63-65* [en línea]. 2013. [Consultado el 20 de septiembre de 2015]. Disponible en: http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1055&context=nslb

CoinDesk. What are Bitcoin Mining Pools? [en línea]. Marzo del 2014. [Consultado el 13 de abril de 2015] Disponible en: http://www.coindesk.com/information/get-started-mining-pools/

- Recursos:

Todos los datos extraídos del valor de las capitalizaciones del Bitcoin y las criptomonedas proporcionados por Coinmarketcap. [Consultado el 22 de febrero de 2016]. Disponible en: https://coinmarketcap.com/

Página oficial del proyecto tor: https://www.torproject.org/

Página oficial del proyecto Bitcoin: https://bitcoin.org/es/

Páginas web oficiales de cada una de las altcoins consultadas en este estudio y sus respectivas wikis:

Ethereum: https://www.ethereum.org/
- Wiki: https://github.com/ethereum/wiki/wiki

Ripple: https://ripple.com/learn/
- Wiki: https://wiki.ripple.com/Main_Page

Litecoin: https://litecoin.org/es/
- Wiki: https://litecoin.info/Main_Page

Dogecoin: http://dogecoin.com/
- Wiki: http://dogecoin.wikia.com/wiki/Dogecoin_Wiki

MaidSafeCoin: http://maidsafe.net/safecoin.html
- Wiki: https://safenetwork.wiki/en/FAQ

PesetaCoin: http://pesetacoin.info/
- Wiki: http://coinwik.org/PesetaCoin

Proyecto dedicado a la explicación de la deep web: http://deep-web.org/

Wiki mantenida por la comunidad Bitcoin: https://en.bitcoin.it/wiki/Main_Page

Revista sobre el estudio de monedas digitales del centro de innovación del BBVA: http://www.centrodeinnovacionbbva.com/innovation-edge/monedas-digitales