UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Facultad de Economía, Empresa y Turismo

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

BITCOIN Y SU USO EN EL COMERCIO MINORISTA ACTUAL EN ESPAÑA

Presentado por: **Beatriz Morales Santana**

Las Palmas de Gran Canaria, a 7 de diciembre de 2015.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLA

I. INTRODUCCIÓN

Hoy en día el mundo de las divisas virtuales es un mundo completamente aparte no es algo nuevo pero muy interesante todo lo que hay detrás. Las monedas virtuales están teniendo un impacto muy significativo en el mundo actual. La divisa que últimamente está acaparando las noticias, es el Bitcoin no es nueva pero si de reciente creación. En este trabajo, vamos a abordar el impacto que tienen las monedas virtuales, especialmente nos centraremos en la moneda Bitcoin. Cómo ha sido el desarrollo de la misma desde sus inicios hasta hoy en día, pasando desde su evolución hasta lo qué se espera conseguir de ella. A simple vista, una moneda no tan reconocida a nivel nacional como puede ser a nivel internacional, analizando para ello las características y el uso que podría tener en nuestro país a raíz de lo que ocurre a nivel mundial.

II. ASPECTOS METODOLÓGICOS

El objetivo de este proyecto se centra en una revisión bibliográfica acerca de la evolución y uso de Bitcoin. Para ello, hemos revisado artículos, libros, vídeos y probado algunas apps desarrolladas para la obtención de *Sathosis*[1]. Aunque la existencia de esta divisa no es nueva y hace tiempo que ya está en el mundo a nivel nacional e internacional, se ha incrementado considerablemente su uso en los últimos tiempos tanto a nivel personal como a nivel empresarial, por lo que resulta interesante estudiar y seguir la evolución de este mercado.

1. Objetivos y justificación

Este trabajo tiene el objetivo principal de analizar cómo ha sido la evolución del Bitcoin y como se está implantando a nivel nacional. Para ello, se explicará primero qué es el Bitcoin así como las funciones básicas importantes para realizar una transacción y sus diversos componentes. Posteriormente, se abordará la manera en que las diversas tecnologías de la información y la comunicación (*TICs*) influyen en los avances de sistema de pagos de Bitcoin,

[1] Satoshi es actualmente la unidad más pequeña de la moneda Bitcoin creada en la cadena de bloque. Es un ciento por millonésima parte de un único Bitcoin (BTC 0,00000001). La unidad ha sido nombrado en homenaje colectivo al creador original de Bitcoin, Satoshi Nakamoto.

además, de los dispositivos móviles que existen actualmente y en los que las aplicaciones móviles llevarán a cabo su función.

Con ello, se pretende dar a conocer la ventaja de utilizar el sistema de pagos de Bitcoin en un negocio para conseguir un mayor beneficio por su utilización.

III. INTRODUCCIÓN AL BITCOIN

1. ¿Qué es el Bitcoin?

Bitcoin[2] es una de las principales criptomonedas[3] desarrolladas que ha tenido éxito en la actualidad. Bitcoin es efectivo electrónico, es decir, es una moneda, pero básicamente digital. Es considerada una divisa muy similar como puede ser el dólar y el euro, pero su característica principal consiste en ser utilizada a través de internet, sin realizar ninguna transacción física, es decir, las transacciones realizadas se llevan a cabo a través de los llamados monederos virtuales, y lejos del sistema financiero tradicional (las tarjetas de crédito y cuentas bancarias no actúan como intermediarios). La creación de esta moneda virtual nació en el año 2009 de las manos de un programador anónimo oculto bajo el pseudónimo Satoshi Nakamoto (Nakamoto, 2008).

Está considerado como el primer ejemplo de criptomoneda utilizada como un medio de intercambio digital. Nakamoto decidió lanzar una moneda electrónica que se caracteriza principalmente por el hecho de que sólo sirve para poder realizar operaciones dentro de la red. Debemos tener muy claro que Bitcoin es básicamente un sistema donde no existe ninguna autoridad central que ejerza el control, por lo que su código es completamente abierto y al basarse en un protocolo P2P[4] (peer to peer), es una divisa completamente descentralizada y muchos la comparan al oro, ya que es un recurso limitado.

---

[2] Bitcoin, para referirse al sistema o el concepto. Y, bitcoin para referirse a unidad monetaria.
[3]Criptomoneda: Una moneda digital que emplea técnicas de cifrado para reglamentar la generación de unidades de moneda y verificar la transferencia de fondos, y que opera de forma independiente de un banco central.
[4] Una red peer-to-peer (P2P) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

A diferencia de la mayoría de otras monedas, el funcionamiento de Bitcoin no depende ni de un gobierno, ni de una entidad financiera, sino de una base de datos distribuida. Es decir, no se puede tocar, pero puede ser utilizada como medio de pago (para realizar intercambios de bienes y servicios) de la misma forma que el dinero físico. El software ideado por Nakamoto emplea la criptografía para proveer funciones de seguridad básicas, tales como la garantía y seguridad de que los Bitcoin sólo puedan ser gastados por su propietario, y nunca pueden ser utilizados más de una vez.

Está representada por la imagen de una “moneda” cuyo signo es: ฿, y su abreviatura es BTC.

A diferencia de un billete o moneda física, no contiene número de serie o cualquier otra referencia que sirva para poder rastrear e identificar a un comprador o vendedor. Esto hace que sea un mercado bastante atractivo para realizar intercambios de bienes o servicios en el mercado negro. Desde hace un tiempo se viene sospechando que está moneda podría estar siendo utilizada también para blanquear dinero.

2. Objetivos y características de Bitcoin

Como se ha podido ir identificando, bitcoin es una moneda bastante novedosa en el mundo virtual, a pesar de llevar no muchos año en uso, es la moneda electrónica más utilizada. No es algo raro ni extraño, ya que cada vez se está haciendo muy conocida a nivel internacional e incluso se está haciendo notar pero en menor medida a nivel nacional. A diferencia de las otras monedas, presenta una serie de características novedosas con una gran serie de ventajas para el usuario, y destacando por su eficiencia, seguridad y facilidad a la hora de realizar los intercambios. A grandes rasgos, esta nueva moneda se puede clasificar básicamente por tres tipos de características:

2.1. Características Económicas

– Las transacciones son irreversibles, es decir, una transacción no puede ser cancelada. La única manera de cancelarla es similar a realizar una devolución por parte del receptor eso sí, de manera voluntaria y mediante una nueva transacción.

- Las transacciones se realizan en cuestión de segundo y la verificación de la transferencia es de aproximadamente diez minutos.
- Se pueden cambiar bitcoin a cualquier moneda o divisa y viceversa.
- Límite de emisión de bitcoin prestablecido, cercano a los 21 millones de bitcoins.

Ilustración 1: Total de bitcoins en circulación

Fuente: https://blockchain.info/es/charts/total-bitcoins

2.2. Características Técnicas

- Los bitcoins se pueden transferir entre nodos[5].
- El doble gasto (uso simultáneo de bitcoin en dos operaciones diferentes) se evita mediante el uso de la cadena de bloques.
- Las transacciones se reciben de manera automática independientemente de si el ordenador de alguno de los usuarios está en funcionamiento o no.
- Los bitcoins son divisibles hasta en ocho posiciones decimales dando un total aproximado de 21x1.014 unidades monetarias.
- Las comisiones por las transacciones son bastante bajas y generalmente suelen ser gratuitas.

[5] Un nodo, en informática, es un componente que forma parte de una red. En otras palabras, tanto si se trata de Internet como de Intranet (utilizada en ámbitos cerrados, con acceso limitado a los usuarios autorizados), cada servidor u ordenador constituye un nodo y se encuentra conectado a otro u otros nodos.

2.3. Características Comerciales

- Es una moneda descentralizada, no es controlada por ningún órgano de gobierno, institución financiera o empresa. Su funcionamiento permite que no sea posible generar inflación a la hora de crear más monedas, sino que es la propia red, mediante la minería (la cual explicaremos más adelante), la que gestiona la emisión de Bitcoin de manera descentralizada y siempre acorde con la demanda en cada momento.

- Prácticamente es imposible su falsificación, debido al sistema criptográfico que la protege, al mismo tiempo que permite simplificar las transacciones realizadas de forma más seguras, ya que son los propios usuarios quienes gestionan su propio monedero.

- No hay intermediarios. Su funcionamiento peer-to-peer (P2P) permite transacciones de forma instantánea, con unos costes bastante reducidos e incluso casi nulos.

- Las transacciones son irreversibles: se trata de una de las características más destacada de dicha moneda, debido a que una vez que se realiza un pago, es imposible que sea anulado.

- No es necesario revelar tu identidad a la hora de realizar negocios y su sistema protege tu privacidad ante cualquier otro usuario.

Desde el punto de vista del usuario, Bitcoin no es más que una aplicación móvil o de escritorio que provee un monedero bitcoin personal y permite al usuario poder realizar las distintas transacciones. Para que Bitcoin cumpla con su principal función, es necesario poder realizar transacciones. Para ello, además de existir un elemento a intercambiar bienes o servicios debe ser posible identificar las diferentes partes que intervienen en una transacción.

En este caso, a la hora de realizar una transacción, el elemento que se va a intercambiar es el saldo de bitcoins, mientras que las distintas partes son reconocidas mediante los identificadores de usuario. Para eso, todos los usuarios tienen que disponer de una serie procedimientos para poder realizar las operaciones y para conocer el saldo que tienen disponible a través de las distintas aplicaciones que se ofrecen.

3. Ventajas

Las principales ventajas que encontramos sobre Bitcoin, las podemos enumerar de la siguiente manera:

- Libertad de pagos: es decir, podrás enviar y recibir sin límites cualquier cantidad de dinero a cualquier lugar del mundo y sobretodo en cualquier momento.

- Comisiones muy bajas: Hoy en día, las comisiones realizadas pueden ser una pequeña cantidad e incluso pueden ser prácticamente nulas. Los usuarios pueden incluir una tasa en sus transacciones para recibir prioridad en su procesamiento, lo que resulta en una confirmación más rápida de las transacciones por parte de la red. Los bitcoin son ofrecidos con tasas mucho más bajas que las que ofrecen PayPal o las tarjetas de crédito, evitándose los comerciantes, las comisiones tanto por las tarjetas de créditos como de débito, como también las comisiones por el cambio de divisa. Lo que suelen hacer los comerciantes, es no poseer ningún balance de bitcoin en sus cuentas. En su lugar, convierten automáticamente cualquier trasferencia que reciben en su moneda local (dólar, euros,…). De esta manera, se reduce el riesgo de volatilidad de los precios.

  Por otro lado, los clientes finales también ahorran dinero, ya que la mayoría de las tarjetas de crédito cobran una cuota anual por dicha tarjeta, cosa que no pasaría con esta moneda virtual. Los mineros que se encargan de verificar dichas transacciones pueden obtener una compensación, el primero que consigue calcular dicho número en la cadena de bloques obtiene como recompensa los 25 bitcoins generados en la última transacción, quedando así registrados todos los movimientos de bitcoin del mundo que se producen durante los diez minutos quedan registrados en un mismo fichero, que se denomina bloque. Por lo tanto, las personas, en este caso los mineros, no reciben ningún pago por la realización de las transacciones. Esto hace que Bitcoin sea sumamente atractivo para ambos, comerciantes y clientes. Sin embargo, la ventaja que posee los bajos costes de transacción puede debilitarse en el futuro. Los beneficios obtenidos por los mineros en las transacciones, está programada que en un futuro puedan estar reducida a la

mitad (cada cuatro años). Por lo tanto, una parte de los costes de la minería correrá a cargo de las personas que llevan a cabo las transacciones en lugar que por la red.

- Menor riesgo para los comercios: Las transacciones Bitcoin son seguras, irreversibles, y no contienen información relevante o personal de los clientes. Esto protege a los comerciantes contra pérdidas ocasionadas por el fraude o devolución fraudulenta, y como hemos visto no es necesario el cumplimiento de las normas PCI DSS (*Payment Card Industry Data Security Standard*).

- Una moneda con restricción de emisión se traduce en deflación de precios, es decir, un aumento decreciente y previsible del valor monetario, lo cual ayuda a garantizar y probablemente a mejorar el nivel adquisitivo de los usuarios de cara a la moneda física, porque el valor de la moneda va hacia la apreciación. Al estar controlado de forma automática el sistema de creación de Bitcoin, esto hace que la oferta de dinero sea limitada, lo que controla la inflación de un modo similar al patrón oro.

- Ofrece un alto nivel de seguridad: cuenta con un fuerte respaldo criptográfico que lo protege de falsificaciones y puede guardarse en múltiples localizaciones a la vez. La tecnología en la que se basa el protocolo del Bitcoin es varias veces más segura que la que utilizan los bancos y las tarjetas de crédito.

- No es necesario cumplir con ningún requisito para poder obtener una cuenta de bitcoin.

- El control de las transacciones es realizado por todos los participantes del sistema, cada operación queda completamente registrada, de tal manera que cualquiera puede ver los movimientos, aunque sin poder detectar quién las hace.

- Las transacciones se hacen en tiempo real, se ejecutan y verifican con un máximo de diez minutos. Cualquier transferencia convencional de dinero de un país a otro suele demandar entre 24 y 72 horas (además de las comisiones) incluso las transferencias internacionales puede tardar hasta una semana. Esta moneda se transfiere en tiempo real de una cuenta a otra y sin

comisiones. Los bitcoins son transferidos directamente de monedero a monedero a través de la red.

4. Desventajas

Son mucho menos las desventajas que esta moneda nos puede ofrecer veamos cuales son:

- Grado de aceptación: Es cierto, que mucha gente no conoce aún Bitcoin. Cada día, más negocios aceptan Bitcoin para aprovechar sus ventajas, pero la lista aún es pequeña y necesita crecer para que puedan beneficiarse de su efecto de red.

- Volatilidad: El valor total de bitcoins en circulación y el número de negocios usando esta moneda virtual son muy pequeños comparado con lo que puede llegar a ser en un futuro. Por lo tanto, esos pequeños intercambios pueden afectar considerablemente al precio. En teoría, esta volatilidad tenderá a decrecer en la medida en la que el mercado y la tecnología de dicha moneda madure con el paso del tiempo, por lo que es muy difícil imaginar que pasará.

- Desarrollo en proceso: El software está en fase beta con muchas características incompletas. Para ello, se están desarrollando nuevas herramientas, características y servicios para hacer Bitcoin más seguro y accesible. Muchos aún no están listos para el público. La mayoría de negocios con Bitcoin son nuevos y no ofrecen seguridad. En general, aún está en proceso de desarrollo.

- Transacciones anónimas: la gran ventaja que se encuentra es que las transacciones realizadas sean anónimas pero a su vez, es una gran desventaja ya que no existe ningún control sobre actividades ilícitas y obligaciones tributarias correspondientes.

- Enorme fluctuación en su valor en comparación contra otras monedas similares. Por lo tanto, determinar el valor de un bitcoin no es una tarea fácil. Se puede meter mucho dinero en todos los tipo de negocios y la compra de Bitcoins puede ser utilizados con fines puramente especulativos.

– No hay garantías de que se convierta en una moneda aceptada por todos. Si la tendencia actual cambiara y los usuarios dejaran de usarla, el valor del Bitcoin se acercaría a cero.

5. Implantación actual del Bitcoin

En la actualidad, existe un número creciente de negocios e individuos usando cada vez más Bitcoin. Esto incluye negocios tradicionales como restaurantes, casas, bufetes de abogados, agencias de viajes y servicios de Internet populares como *Namecheap, Wordpress, Reddit y Flattr*. Algunos ejemplos de e-commerce que ya usan bitcoins en España son la agencia de viajes *Destinia*, el Hotel *One Shot Recoletos* y decenas de tiendas ubicadas en las principales calles comerciales de Madrid, Barcelona o Valencia. A nivel internacional destacan nombres tan conocidos como *Dell, Wikimedia Foundation, Google, WordPress o Square.* Pero, aunque Bitcoin sigue siendo un fenómeno prácticamente nuevo, está creciendo muy rápido. A finales de Agosto de 2013, el valor de los bitcoins en circulación superaba los 1.5 billones de dólares[6] y cada día se intercambiaban el equivalente a millones de dólares en bitcoin.

El número de descargas por volumen de pagos del programa Bitcoin, también llamado *Bitcoin-Qt* o *cliente Satoshi*, por países que más uso hacen desde su lanzamiento hasta el 31 de octubre de 2015 es:

	2010	2011	2012	2013	2014	2015	Total
United States	16.329	346.820	244.669	736.720	98.586	12.276	1.455.400
China	676	71.758	24.817	584.389	97.806	981	780.427
Germany	1.812	98.790	46.590	153.747	45.072	9.202	355.213
Russia	7.404	54.641	52.510	163.307	39.962	2.227	320.051
United Kingdom	2.588	54.550	51.292	159.702	20.576	1.273	289.981
Canada	2.625	45.083	32.805	113.654	16.483	715	211.365
Netherlands	994	23.931	19.459	77.137	9.264	827	131.612
Australia	1.290	25.430	23.317	68.478	8.179	440	127.134
Poland	987	33.981	18.210	62.097	10.360	357	125.992
France	1.552	19.771	12.019	60.469	14.989	1.339	110.139
Greece[7]	220	3.111	4.145	13.122	1.579	119	22.296

Adaptado de la fuente http://sourceforge.net/ desde el 31 de enero de 2010 hasta el 31 de octubre de 2015.

[6] Billones en dólares son miles de millones en euros.
[7] Además de incluir los países que más lo utilizan hemos querido también tener en cuenta a Grecia debido a los últimos acontecimientos que ha tenido lugar con esta moneda.

6. Requerimientos técnicos para su implantación

Uno de los aspectos más importantes a la hora de usar una aplicación Bitcoin es su seguridad. Para garantizarlo se utilizan los monederos (*wallet*), un espacio virtual, similar a un monedero físico, donde se almacenan y gestionan direcciones Bitcoin de un usuario y los pagos que se realizan con ellas. Los monederos pueden ser online y offline. Las online son más sencillas de crear y las offline son más seguras, pero más complicadas de manejar.

Todos los monederos funcionan con una criptografía de clave pública. Esto quiere decir que hacen falta dos elementos para verificar la firma y administrar o modificar los datos del monedero: una clave pública (la dirección de destino de bitcoins en el caso de un envío) y una parte privada que debe estar en posición del usuario de BTC.

Bitcoin es en realidad un archivo que necesitamos para enviar y recibir bitcoins; puede decirse que este archivo "*contiene*" nuestros bitcoin, aunque lo que contiene principalmente son llaves criptográficas (claves privadas, únicas, irrepetibles y secretas) que nos hacen propietarios de nuestros Bitcoin y nos permiten autorizar pagos. Cabe destacar que existen diferentes programas de utilización de Bitcoin como pueden ser *Electrum*[8]*, BitcoinCore*[9]*, MultiBit HD*[10]*, Bitcoin Wallet Armory*[11]*, Mi monedero de Blockchain.info*[12]*…* o simplemente un monedero de papel.

El monedero se puede tener en varios dispositivos en forma de copias de seguridad, por lo que si por error se borra del sistema operativo o el ordenador se ve afectado por un *malware*[13], el usuario no pierde sus bitcoins. Sin embargo, la clave privada se puede apuntar en un papel y guardar en lugar seguro (*paperwallet*) o se puede generar a partir de una frase convenientemente segura que el usuario siempre lo recuerde (*brainwallet*). Si, por ejemplo, todas las copias

[8] *Electrum*: https://electrum.org/
[9] *BitcoinCore*: https://bitcoin.org/es/
[10] *MultiBit HD*: https://multibit.org/
[11] *Bitcoin Wallet Armory*: https://bitcoinarmory.com/
[12] *Monedero de Blockchain*: https://blockchain.info/
[13] Malware: es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

de seguridad de tu monedero se pierden y la clave se olvida, el monedero quedaría inaccesible. Lo mismo ocurre, si una persona obtiene la clave de otra persona puede tener acceso a su cuenta y ordenar transferencias de manera totalmente anónima. El uso directo de Bitcoin a través de uno o varios monederos es igual al uso de dinero en efectivo. Tenemos que tener claro que, este sistema de Bitcoin sea similar al uso de efectivo no significa que se limite a únicamente a eso.

Si el uso del sistema terminara por generalizarse y empezara a utilizarse como dinero surgirían múltiples instituciones prestando diversos servicios y productos financieros en torno a Bitcoin. Los usuarios podrían elegir entre usar el sistema integrado de Bitcoin o confiar la gestión de su dinero a una entidad financiera.

IV. CONCEPTOS BÁSICOS PARA EL USO DE BITCOIN

1. Identificación del monedero

Una dirección Bitcoin, el cual es equivalente a un monedero, es una cadena de caracteres, cuya extensión es habitualmente de 33 caracteres (aunque puede oscilar entre 27 y 34 caracteres) en el cual puede haber o ha habido en el pasado un número determinado de bitcoin. Una dirección se forma a partir de dos parámetros: la versión del protocolo (v) y una clave pública (pk) del algoritmo ECDSA[14]:

1. hash_key = v || RIPEMD160(SHA256(pk))
2. checksum = SHA256(SHA256(hash_key)) y sólo cogiendo los primeros 4 bytes del resultado
3. address = Base58Enc(hash_key || checksum)

Ilustración 2: Proceso de generación de una dirección Bitcoin.

Solo el propietario de la clave privada puede relacionarse con la clave pública y mediante su clave puede desbloquear el uso de los fondos depositados en su

[14] Elliptic Curve Digital Signature Algorithm (ECDSA) es un algoritmo criptográfico utilizado por Bitcoin para asegurar que los fondos sólo pueden ser gastados por sus legítimos propietarios. Es una variante del Digital Signature Algorithm (DSA) que utiliza la criptografía de curva elíptica (Elliptic Curve Cryptography – ECC) como variante de la criptografía asimétrica o de clave pública.

dirección. Al final del proceso, el usuario obtiene una dirección (*address*) codificada mediante un algoritmo ECDSA.

Aunque el formato original es una cadena de caracteres codificada, las direcciones también se pueden presentar con otros formatos distintos, como por ejemplo mediante un código QR.

Ilustración 3: Código QR dirección 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Fuente: http://bitcoinqrcode.org/

Dado que las transacciones en Bitcoin son totalmente públicas, cualquiera puede determinar el contenido (actual o pasado) de una dirección en concreto, así como enlazar las transacciones en las que ha participado una misma dirección, aunque no se pueda relacionar quién es el propietario de dicha dirección. Para evitar en todo momento que se puedan enlazar diferentes transacciones con una misma dirección, es buena no usar la misma dirección más de una vez, por lo que se recomienda que las direcciones no se reutilicen para realizar varias transacciones.

2. Cadena De Bloques

Los bitcoins se encuentran en lo que se denominan "*bloques*", que se generan entre todos los nodos de la red. Un bloque es un registro en la cadena de bloques que contiene confirmaciones de transacciones pendientes. Aproximadamente cada diez minutos, se crea un nuevo bloque que incluye nuevas transacciones, las cuales, se incluye a la cadena de bloques a través de la minería.

La cadena de bloques es el núcleo central de Bitcoin y consiste en la lista de todas las operaciones realizadas con Bitcoin hasta la fecha una vez validadas. Es un registro público de todas las transacciones que se hacen mediante Bitcoin en orden cronológico y encadenado, ya que el cierre de cada bloque origina uno nuevo, mediante un cálculo matemático secreto. Se trata de un fichero que con el tiempo se va haciendo cada vez más largo a medida que se incorporan nuevas transacciones.

El primer bloque creado fue el llamado "*Bloque Génesis*", sobre el que se fue construyendo la cadena. Dicho bloque tenía una recompensa de 50 bitcoins, llamada *Coinbase* para las recompensas de los nuevos bloques. Dicha recompensa la recibió la dirección pública de bitcoin que se observa en la Ilustración 2. Está se comparte entre todos los usuarios de Bitcoin. La cadena de bloques es el único elemento a partir del cual se puede determinar el saldo de un usuario. Aproximadamente seis veces por hora, la red Bitcoin crea y distribuye un nuevo bloque de Bitcoin. La cadena de bloques es uno de los aspectos más cuestionados en lo que respecta al anonimato del sistema, dado que la información de todas las transacciones se almacena sin ningún tipo de cifrado y de forma accesible para todos los usuarios.

Actualmente, la dirección en la cual que se generó el primer bloque (Bloque Génesis) de la red P2P Bitcoin tiene un total de 65,39125463 BTC (alrededor de 21.000 dólares al cambio actual), y la última transferencia fue recibida el 19 de noviembre 2014.

Ilustración 4: Número de transacciones por Bloque.

Fuente: https://blockchain.info/es/charts/n-transactions-per-block

3. Obtención de Bitcoin

Los bitcoins hoy en día son fáciles de obtener. En primer paso es obtener un monedero y a partir de ahí algunos de los mecanismos por los que se pueden obtener bitcoins pueden ser los siguientes:

3.1. Minería

Los bitcoins son generados mediante un proceso competitivo y descentralizado llamado "*minería*". ¿Qué es la minería? Se denomina "minería de Bitcoin" al proceso de generación de bloques, los cuales son incorporados en la cadena de bloques y de esta manera se procesan y verifican las transacciones. A su vez, constituye el mecanismo único por el que se ponen en circulación los nuevos Bitcoin. Cualquier usuario que cumpla con los requisitos y exigencias puede convertirse en un minero.

La minería de Bitcoin ofrece una recompensa a los generadores de los bloques, por un lado, se están beneficiando de los Bitcoin que se les otorga por la creación del bloque, así como por las comisiones que pudiesen haberse obtenido por parte de algunas transacciones que quieren asegurarse estar en el siguiente bloque.

Cuantos más mineros acceden a la red, incrementa la dificultad para obtener beneficios y por lo tanto, deben buscar la mayor eficiencia para reducir sus costes operativos. Ninguna autoridad tiene el poder de controlar o manipular el sistema para aumentar sus beneficios. Cada Bitcoin que hay en el mundo rechazará de forma automática todo lo que no se ajuste a las normas que se esperan del sistema a seguir.

3.2. Otros medios

– Compra en servicios de intercambio que están apareciendo en la red. Los más utilizados son *BitStamp*[15] y *BTC-e*[16]. Pero hay muchos otros sitios que facilitan el intercambio de todo tipo de divisas por bitcoins y admiten diversos sistemas para transferir los fondos.

[15] *BitStamp: https://www.bitstamp.net/*
[16] *BTC-e: https://btc-e.com/*

– Intercambio entre particulares.

– Aceptar bitcoins como pago por bienes o servicios. Es posible fijar un precio en cualquier moneda y optar por ajustar automáticamente los precios nominados en bitcoins. Por medio de *BitPay*[17], los pagos en bitcoins además pueden ser automáticamente convertidos a la moneda que el comerciante prefiera

– Sitios que aceptan pagos por medio de Western Union.

– Compensación por la venta de productos o servicios.

– Involucrarse en la minería de Bitcoin.

– Juegos (*faucet*[18]) basados en Bitcoin que obsequian porciones de bitcoin, como *Dragon's Tale* (MMORPG), *Strike Sapphire* (casino) o *Seals with Clubs* (póker). Aplicaciones obtenidas a través de Play Store (Google) o App Store (Apple).

Sin embargo, también es posible encontrar individuos que desean vender Bitcoin a cambio de un pago por PayPal o tarjeta de crédito, importante saber que la mayoría de las casas de cambio de monedas no permiten utilizar estos sistemas de pago. Esto se debe a que alguien compra Bitcoin con PayPal y luego revierte la mitad de su transacción. Esto es conocido como reembolso e incluso una cantidad mayor.

4. El precio del Bitcoin

A diferencia del dinero *fiat*[19], el precio del Bitcoin se establece en función de la oferta y la demanda. Cuando la demanda de Bitcoin se incrementa, el precio sube, y cuando la demanda disminuye, el precio desciende. Hay un número

[17] *BitPay*: https://bitpay.com/

[18] Los *faucet* son páginas que regalan bitcoin, como modo de promocionar el uso de esta moneda. Es un modo de ganar Sathosis. En este tipo de páginas podemos ganar diferentes cantidades de bitcoin por solo introducir nuestra dirección de monedero y resolver un captcha.

[19] Dinero "*fiat"* Se le llama así, al dinero que no promete la entrega ni de oro, ni de plata, ni de ninguna otra cosa, al portador del mismo. Hace referencia al dinero cuya principal característica es el respaldo legal, a menudo se utiliza de forma intercambiable con dinero fiduciario, ya que el dinero basado en deuda suele coincidir en tener a su vez respaldo legal, sin embargo, los términos no son equivalentes y el matiz puede ser considerable.

limitado de Bitcoin en circulación y los nuevos Bitcoin son creados a una velocidad predecible y decreciente. Bitcoin es finito, y se sabe siempre cuando dinero hay en circulación, por lo que, el número de Bitcoin creados cada año se reduce a la mitad de forma automática a lo largo del tiempo hasta que la emisión de Bitcoin se detenga por completo hasta llegar a los 21 millones de bitcoins. No obstante, esto nunca será una limitación pues los bitcoins pueden dividirse hasta en 8 cifras decimales, es decir, cada bitcoin es divisible en cien millones de partes (0,00000001 BTC) a esta parte, que son la unidad mínima del sistema se le denomina *Satoshi*.

Esto hace que sea un negocio muy competitivo, por lo que, que la demanda debe seguir este nivel de inflación para mantener un precio estable. Debido a que Bitcoin es todavía un mercado relativamente pequeño comparado con lo que podrá llegar a ser, no es necesaria una significativa cantidad de dinero para mover el precio del mercado arriba o abajo, es por eso que el precio del Bitcoin es todavía muy volátil.

Ilustración 5: Evolución del precio de un bitcoin respecto al dólar en el Exchange BitStamp.

Fuente: http://www.bitcoincharts.com

Ese pico importante que podemos observar en la Ilustración 5, que se produjo exactamente el 29 de noviembre de 2013, es debido a la especulación de la moneda, en ese periodo llego a alcanzar los 1.132,26$. Sin embargo, "*A principios del 2014, bitcoin saltó a las noticias precisamente por los elevados precios superiores a 1.200 dólares que alcanzó. Estaba siendo fruto de la especulación, y al no tener una autoridad central que pudiera frenarla, ésta se había desmadrado"* comentaba Víctor García, de *Cripto-Pay*[20]*. "La volatilidad fue*

[20] *Cripto-Pay: https://cripto-pay.com/*

alta, desde luego muy superior a la de una divisa tradicional, aunque desde el pasado otoño las fluctuaciones fuertes han parado y en este 2015 tenemos una moneda muy estable, con tendencia al aumento de valor" (Moratalla, 2015).

5. Métodos de transacciones.

Las *"cuentas*" de bitcoin no contienen en ellas el nombre de las personas y no necesariamente corresponden específicamente a individuos. Es decir, se envían desde y hacia monederos Bitcoin electrónicos, y están firmadas digitalmente para garantizar su seguridad, todo el mundo en la red sabe que se ha hecho una transacción, y la historia de una transacción puede ser rastreada hasta el punto donde se produjeron los bitcoin.

Para componer una transacción se necesitan los siguientes componentes, formando la estructura que se muestra en la siguiente figura:

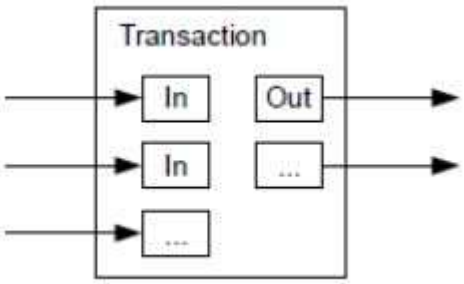


Ilustración 6: Estructura de una transacción con inputs y outputs.
Fuente: **"***Bitcoin: A Peer-to-Peer Electronic Cash System*", Satoshi Nakamoto.

- Entrada o *Inputs*: es una referencia a un output de una transacción anterior, es decir, son registros que referencian los fondos de transacciones previas.

- Cantidad**:** número de bitcoins que se envían.

– Salidas u *Outputs*: contienen instrucciones para enviar un número determinado de bitcoins, es decir, son registros que determinan el nuevo propietario de los bitcoins transferidos.

Ilustración 7: Número de transacciones por día de Bitcoins.
Fuente: https://blockchain.info/es/charts/n-transactions

A continuación, veremos un ejemplo de transacción tanto, desde el punto de vista interno (como funcionada entre la red) como externo (como lo vería el usuario).

Ilustración 8: Ejemplo de transacción externo.
Fuente: www.blockchain.com


```
{
"hash":"ca4b16a1684eeb1cdc6d8b13f3c21b549b7091fdc62b541c90e37ebecf1a9fa2",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":226,
"in":[
  {
    "prev_out":{
      "hash":"11ab99409413b4733e43bed6d7771073567d0f92988875205ab930b7fb5b364c",
      "n":0
    },
    "scriptSig":"30450220654d5327e9d532753779d9190833349b2cfc0851d584c32c945b4e7d6fc47574022100deb6b41d4[...]"
  }
],
"out":[
  {
    "value":"0.61650000",
    "scriptPubKey":"OP_DUP OP_HASH160 2b0d981dfaf5e97eb70ad54356d21c8753bfe768 OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value":"0.11189000",
    "scriptPubKey":"OP_DUP OP_HASH160 0287fa0e7eb4c45e67167296899a30c03c755893 OP_EQUALVERIFY OP_CHECKSIG"
  }
]
}
```


Ilustración 9: Ejemplo de transacción interno.
Fuente: www.blockchain.com

En la Ilustración 9, se puede observar un ejemplo de una transacción desde el punto de vista interno, realizada desde una dirección a dos direcciones independientes.

Existe un tipo especial de transacción llamada transacción base (*coinbase transaction)* que no contiene ningún input. Este tipo de transacciones otorgan una cierta recompensa al nodo que posee la dirección que ha resuelto un bloque. Aunque no tenga ningún input, puede tener un número arbitrario de outputs en caso que la recompensa se deba dividir entre diferentes direcciones. Además de la recompensa fija por resolver el bloque, el usuario también recibe la cantidad correspondiente a las comisiones (*transaction fees*) especificadas en cada una de las transacciones agregadas en el bloque que se acaba de resolver.

La verificación de dichas transacciones se ejecuta de forma establecida a lo largo de la red P2P, de modo que todas las transacciones se anuncian de forma pública y todos los participantes deben de ponerse de acuerdo en un único historial de transacciones. Debido a la inexistencia de entidades centrales o bancos que verifiquen la línea temporal de las transacciones (ordenadas cronológicamente) y para verificar que la transacción que se ha realizado no se ha gastado previamente (*double-spendings*).

5.1. ¿Cómo se envía el dinero?

Recordemos que para poder realizar las distintas transacciones se necesitan dos cosas: una dirección Bitcoin y una clave privada. Como hemos explicado, la clave privada es otra secuencia de letras y números, pero a diferencia de su dirección Bitcoin, esta se mantiene en secreto.

Cada entrada es firmada digitalmente por el comprador, lo que desbloquea los fondos contenidos en la dirección asociada a la clave privada utilizada para firmar. Así, el usuario que posee la clave privada correspondiente es capaz de crear una firma válida, lo que confirma que él es el propietario del saldo y puede utilizarlo.

En las salidas se especifica, entre otros datos, la dirección del cliente que recibirá los bitcoins y, en caso necesario, una dirección en propiedad del deudor para recibir la vuelta.

En una transacción, la suma de sus *inputs* debe ser igual o mayor que la suma de las *output*. En el caso de que la cantidad de bitcoins de los *inputs* sea mayor que el de los *output*s, la diferencia se considera una tasa de transacción o también denominada comisión, y quien incluya esa transacción en la cadena de bloques puede disponer de esa cantidad. Cuanto mayor sea ese coste de transacción (comisión), menor será el tiempo que la red tarde en confirmar la misma, ya que las transacciones con mayor tasa de transacción se suelen mover más rápidamente por la cola de espera de transacciones pendientes de confirmación.

Esta recompensa es una manera de motivar a los mineros, que obtienen beneficios por su trabajo en forma de Bitcoin, siendo los pagadores los que suelen establecer la tasa a incluir en sus pagos.

Se debe tener en cuenta que la recepción de un pago es casi instantánea con Bitcoin. Sin embargo, hay un retraso de diez minutos de media antes de que la red empiece a confirmar esa transacción, al incluirla en un bloque, y antes de que se puedan gastar los Bitcoin recibidos. Una confirmación significa que hay un consenso en la red en que los Bitcoin recibidos no han sido enviados a alguien más y son ahora de tu propiedad. Por otro lado, algunos comerciantes no tienen que esperar, ya que reciben lo generado sin necesidad de saber que la transacción se haya confirmado, esto sucede a menudo en las transacciones donde el riesgo de fraude no es muy grande.

V. BITCOIN Y EL COMERCIO MINORISTA

El sistema de pagos utilizados por Bitcoin es muy similar al sistema de pagos electrónicos que utilizamos diariamente. Sin embargo, este último, basado en el pago con tarjetas de crédito, transacciones bancarias, PayPal, etc., sí está regulado por la ley. Por ejemplo, en el caso de que se incumpla un pago o no se entregue un producto adquirido mediante tarjeta, se puede reclamar ante la administración pública, algo que no sucede si la transacción se realiza con Bitcoin.

Con el crecimiento actual del sistema Bitcoin en la actualidad, más y más comerciantes, incluso de pequeñas empresas, empiezan a aceptar dicha moneda como un medio de pago para la venta de bienes y servicios. Cabe destacar que hace varios años, era casi improbable por no decir imposible, encontrar un comerciante que aceptara el pago en Bitcoin, pero hoy en día, es cada vez más creciente incluso que las empresas a nivel internacional las reconozcan como un medio de pago, pero también es posible ver Bitcoin en comercios tradicionales a pesar del riesgo que se les puede representar.

Esto está haciendo que muchas empresas del sistema financiero nacional estén optando por invertir en esta moneda virtual. El primer establecimiento bancario en España que decidió invertir fue Bankinter. Esta entidad invirtió en la compañía *Coinffeine*[21], cuyo capital está constituido por Bitcoin, una compañía emergente (*startup*) española pionera por desarrollar una plataforma de software que permite el intercambio de divisas y Bitcoin entre personas, de manera descentralizada, segura y anónima, y sin que los usuarios tengan que ceder la gestión de su dinero a un tercero de confianza., y lo hizo a través de su Capital Riesgo. Este movimiento convirtió a Bankinter en el primer banco español que decide introducirse en el negocio de las monedas digitales. Posteriormente también, el Banco BBVA, que invirtió a través de su proyecto de capital riesgo *BBVA Ventures* en la compañía *Coinbase*[22], una plataforma de Bitcoin para realizar transacciones con la divisa virtual Bitcoin, que se utiliza como monedero virtual (*wallet)*. A principios del año 2015, *Coinbase* contaba con 2,1 millones de

[21] *Coinffeine:* http://www.coinffeine.com/es/
[22] *Coinbase: https://www.coinbase.com/*

consumidores que usan su cartera virtual, 38.000 negocios que procesan pagos con Bitcoin a través de su plataforma y 7.000 desarrolladores que construyen nuevos servicios basados en su interfaz de programación de aplicaciones (*API*).[23]

A pesar de los riesgos que puede poseer esta moneda, cada vez más son los sitios en internet que aceptan esta moneda virtual como forma de pago. Además le facilita mucho el hecho de poder realizar distintas transacciones entre particulares y comercios a través de diversas aplicaciones en dispositivos móviles.

Desde el año 2013 hasta la actualidad, en España se están estableciendo en pequeños y grandes comercios, incluso de amplio reconocimiento a nivel internacional, que acepta como medio de pago Bitcoin en su establecimiento. Pese últimamente, a la publicación de artículos acerca de relación existente con el mercado negro, se está observando cómo esta moneda está entrado en nuestro sistema, pese a no estar centralizada.

En España, Madrid tiene la Calle Bitcoin más larga de Europa, se ha implantado en la famosa "*Milla de Oro*" de la capital madrileña, en la zona comercial por excelencia de la Calle Serrano. Entre los comercios, el usuario que disponga de Bitcoins puede realizar sus compras en tiendas como Agatha Ruiz de la Prada, el centro comercial ABC Serrano o en Bucarelli o alojarse en el hotel One Shot Recoletos 04, donde además se encuentra un cajero de bitcoin.

En cuanto a restaurantes y cafés, destacan The Geographic Club, La Castela, de comida casera o Do-Eat, el primer restaurante Bitcoin de Madrid. Tampoco faltan otros comercios con servicios diversos como puede ser: de arquitectura, como Ana Muñoz González, de abogacía, como F&J Martín Abogados e incluso de ginecología, como la consulta del doctor Emilio Santos (ver Anexo III).

La pregunta que muchos se estaban haciendo en esos momentos es ¿Qué hace una moneda digital como está en un sitio como este? Esta iniciativa surgió de un

[23] *Application Programming Interface* (API) es un conjunto de reglas (código) y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas: sirviendo de interfaz entre programas diferentes de la misma manera en que la interfaz de usuario facilita la interacción humano-software

grupo de seguidores de la moneda bitcoin que estaban trabajando para conseguir que las tiendas comenzaran a aceptar Bitcoin como medio de pago *"con el objetivo de lograr que los distintos comercios se animaran a usarla. Principalmente en Madrid hay establecimientos que la acepta pero que se encuentran dispersas geográficamente. Su objetivo era que un elevado número de tiendas cercanas en una zona concreta aceptaran esta moneda para así poder llamado "Bitcoin Boulevard",* según comentaba Álvaro Gómez, uno de los promotores de esta iniciativa y CEO de la *startup* española *Coinffine* (Á. Hernández, 2015). Para los comerciantes supone un gran avance respecto a las tarjetas de crédito tradicionales, ya que no tiene ningún coste de comisiones. Principalmente para poder empezar a utilizarlo en un comercio es tan sencillo como tener el código QR de su cuenta para que el comprador realice su envío de dinero. Este código sólo permite el ingreso, pero no la retirada, por lo que no hay ningún problema con que sea visible para el público. Una simple operación que podría ayudar a los comerciantes en el futuro a ampliar su capacidad de aceptación de medios de pago.

Con el paso de los años, este sistema ha ido evolucionando más despacio en comparación con otros países por la falta de información y la desconfianza de los usuarios, pero en el 2014 se fundó *ATM Bitcoin España, S.L*., para llevar a cabo la comercialización, desarrollo y difusión de las criptomonedas digitales, especialmente Bitcoin, instalando los primeros cajeros automáticos para comprar y vender Bitcoin, directamente y sin intermediarios.

Por otra parte, y algo más reciente, ha surgido otra *startup* española conocida como *Bit2Me*[24], que propone la posibilidad de a través de su aplicación en tu dispositivo móvil, indicar la cantidad de bitcoins que queremos cambiar y recibir a cambio de nuestro dinero casi al momento. Todo ello mediante un *hal-cash*[25] que envía un código con la cantidad deseada de dinero a la dirección que nos proporcionan y acto seguido podemos ir a recoger nuestro dinero a cualquier de los cajeros compatibles. Actualmente, el número de establecimientos financiero que permiten realizar estas operaciones son casi 10.000 los que disponemos

[24] *Bit2me*: https://bit2me.com/es/

[25] *Hal-cash*: es un servicio bancario que le permite enviar dinero a cualquier persona a su teléfono móvil de manera inmediata. Ellos podrán retirarlo desde el mismo instante en que reciban la orden *Hal-Cash*, en un cajero sin ser cliente del banco ni usar tarjetas de crédito.

solo en España bajo la insignia de Bankinter, ING Direct, Banco Popular, Caja Laboral, EVO Bank, Abanca o Cajamar.

Sin embargo, la pregunta principal que hasta el momento, ha centrado el mayor interés en relación con los Bitcoin (BTC), es el tratamiento en el IVA de sus operaciones de compraventa en España, aunque según ha publicado recientemente por el Tribunal Superior de Justicia de la Unión Europea ha dictaminado que tanto Bitcoin como otras monedas virtuales estarán exentas de comisiones. La Dirección General de Tributos (en adelante DGT) considera que los Bitcoin son un medio de pago y que por las características que presenta, su transmisión está exenta del impuesto sobre el valor añadido. La explicación que daba la DGT a una publicación realizada en 30 de marzo del 2015, es que "*las monedas virtuales Bitcoin actúan como un medio de pago y por sus propias características deben entenderse incluidas dentro del bloque del concepto 'otros efectos comerciales' por lo que su transmisión debe quedar sujeta y exenta del impuesto"* (Martín Fernández, 2015).

Los últimos avances sobre esta moneda, es que se están impulsado la aparición de nuevas formas de pago tanto en el comercio electrónico como en los comercios físicos. Aparte de los cajeros que ya están implantado, se están realizando acuerdos muy recientes entre la empresa *Ingenico*[26] y *BitPay,* que ha puesto en marcha el novedoso proyecto permitir a los comerciantes aceptar Bitcoin a través de un TPV convencional. Esto estará implementando en un futuro muy cercano ya se están probando los primeros dispositivos con el sistema beta pero todavía no podemos saber a ciencia cierta cómo podrá funcionar en los establecimientos (Merino, 2015). Esta innovación tecnológica supondrá un incentivo para el uso de esta moneda virtual mediante el pago físico a través de una tarjeta. Un ejemplo real de tarjeta de débito, lo encontramos es *Xapo*[27] que se encuentra vinculada a nuestro monedero virtual. Todavía a España no ha llegado a comercializarse este tipo de tarjetas de débito, pero en un futuro observando las posibilidades de cómo el mercado se está desarrollando a nivel global, se encontrara muy próximo en llegar.

[26] *Ingenico: http://www.ingenico.es/*
[27] *Xapo: https://xapo.com/*

Actualmente, se está utilizando en España, la tarjeta *E-Card (*versión beta*)* de *E-Coin*[28], funciona exactamente igual que otra tarjeta de débito que puedas tener. La única diferencia es que permite pasar bitcoins en cualquier lugar dentro de la red VISA, se pueden transferir los fondos de bitcoin que posee en su monedero e inmediatamente tenerlos en su *E-Card*. Los beneficios asociados a esta tarjeta son:

- Carga instantánea en la cuenta de E-Coin.
- Utilizar los bitcoins para comprar artículos a través de minoristas, tanto online como en tiendas físicas en todo el mundo.
- Retirar dinero en efectivo a través de la red ATM que abarca más de 200 países.

Como toda tarjeta, posee ciertos límites, y también hay que tener en cuenta que esta tarjeta tiene una validez de un máximo de tres años.

1. Evolución de la implantación del Bitcoin

Una de las cosas más importantes a tener en cuenta sobre la tecnología bitcoin para los comerciantes es que está precisamente unida a la 'moneda' bitcoin. Se argumenta que la mayor parte de los beneficios de Bitcoin para los comerciantes tiene que ver con el sistema de pagos, pero también la moneda en sí resulta prometedora.

La primera opción para aceptar bitcoin en nuestro establecimiento es que esta moneda está libre de fraude, cosa que no ocurre con las tarjetas de crédito, el riesgo que poseen es que pueden ser robadas. En cambio con bitcoin desde la perspectiva de fraude es similar a mantener el efectivo, no hay una tercera parte involucrada en la transacción. Aceptar bitcoin ofrece una gran cantidad de beneficios tanto para los comerciantes como para los consumidores. Por un lado, para los comerciantes posen una tarifa de comisión más bajas por transacción

[28] *E-Coin: https://www.e-coin.io/*

de (1,2%) frente a la mayoría de otros sistemas de pago en línea, por otro lado, para el consumidor, no se cobran comisiones por transacción.

Además, esto no supone un problema tecnológico ya que hay empresas como *Coinbase* y *BitPay* que hacen más fácil aceptarlos gracias a sus desarrolladores API que permiten la conversión de bitcoin en su moneda local con un riesgo de conversión de cero.

Otra cosa a destacar es que el uso de bitcoin será una oportunidad ideal de internacionalización de nuestro negocio, ya que permite a los clientes de cualquier parte del planeta comprar sus productos sin tener que preocuparse de si acepta la moneda de su país, de esta forma, aumentaríamos nuestra cartera de clientes.

VI. TENDENCIA DEL BITCOIN

El dinero tal y como lo conocemos tiene los días contados: las formas de pago electrónico desbancaran a lo que conocemos como billetes y monedas. En el caso de Bitcoin ha sido un experimento de criptografía que ha alcanzado unas proporciones inesperadas. Una moneda que en menos de doce meses ha llegado a alcanzar los 400 dólares, y que en cualquier momento puede tener fluctuaciones de precio, muchos consideran que no es una divisa tranquilizadora. Porque a día de hoy, se plantea si esta moneda podría tener futuro o es una burbuja.

Pero cada vez son más los negocios que aceptan el Bitcoin como una forma de pago. Desde las exclusivas tiendas ubicadas en la milla de oro madrileña hasta las casas de juego, lotería y apuestas online. Según Jeff Garzik, desarrollador de la criptomoneda, "*en un futuro pagaremos con bitcoins sin saberlo*" (Benavente, 2014).

Otro aspecto a tener en cuenta, es que la máxima autoridad judicial de la Unión Europea ha declarado que las operaciones realizadas con bitcoins están exentas de tributación en toda la unión monetaria en "*virtud de la disposición sobre operaciones relativas a las divisas, los billetes de banco y las monedas que sean medio legal de pago"* (Tribunal de Justicia de la Unión Europea, 2015).

Recientemente se ha comenzado a hablar de las relaciones existentes entre *Coinbase* uno de los principales exchange de Bitcoin y *Shift Payments*[29] para el lanzamiento de *Shift Card*, una tarjeta de débito VISA que por ahora solamente permitirá a los habitantes de Estados Unidos podrán pagar online y offline con bitcoins en más de 38 millones de comercios en todo el mundo. El sistema de *Shift Payments* funciona de la siguiente manera: cuando los usuarios utilicen su tarjeta para realizar alguna compra, el valor equivalente en bitcoins se deducirá de su monedero de acuerdo con el tipo de cambio vigente en ese periodo que es lo que recibe el comerciante. Para obtener una tarjeta de *Shift* los usuarios de *Coinbase* deben proporcionar su identidad y autorizar el pago de una cuota de emisión de 10$. Por el momento, las operaciones nacionales en Estados Unidos serán gratuita, mientas que para usar su tarjeta en el extranjero, los usuarios deberán pagar una comisión del 3% (A. Hernández, 2015).

VII. CONCLUSIÓN

Como se sabe, el mundo de la tecnología está evolucionando a un ritmo acelerado y todo apunta a que seguirá siendo así en los próximos años. Vemos cómo, prácticamente esta moneda en menos de seis años ha evolucionado de manera inesperada y enorme, con una capitalización de mercado increíble de imaginar. Pero cada vez es mayor la demanda de transacciones de bitcoins y esto plantea un gran problema. Se están desarrollando numerosos cambios en el protocolo de *blockchain* lo que permitirán un mejora en el rendimientos la hora de confirmar las transacciones en cuestión de segundo y no en minutos.

En el presente trabajo hemos estudiado la naturaleza del Bitcoin. Partiendo de su origen, hemos discutido las características principales de esta moneda. En él, hemos incluido como funciona a través de internet, así como haciendo referencia a su estructura criptográfica. El modo con el que las operaciones comerciales tienen lugar mediante el Bitcoin ha sido objeto de estudio a lo largo del presente trabajo. La generación de la moneda (minería) y su extendido uso comercial, con particular importancia en su naturaleza P2P y la imposibilidad del doble uso, han sido analizados. Así como también sus ventajas y desventajas. Creemos que el

[29] *Shift Payments: https://www.shiftpayments.com/*

uso de los bitcoins es útil para el comercio, aunque estamos a la espera de una nueva evolución que afectara a nivel global, ya que ha sido acogido bastante bien por parte de los usuarios. Por lo que se refiere al comercio, el uso del Bitcoin en las transacciones comerciales se está extendiendo a gran ritmo y el número de comercios que aceptan esta moneda crece día a día. En definitiva, se ha intentado dar a conocer la evolución del sistema que engloba Bitcoin y cómo se ha ido implantado en España. Con la revisión bibliográfica llevada a cabo se ha podido aprender y corroborar todo lo dicho anteriormente, sirviendo de gran ayuda ya no solo para el trabajo sino también a nivel personal.

VIII. REFERENCIAS

Benavente, R. P. (2014). “En el futuro pagaremos con ‘bitcoins’ sin saberlo.” Retrieved from http://www.elconfidencial.com/tecnologia/2014-11-16/en-el-futuro-pagaremos-con-bitcoins-sin-saberlo_455649/

Hernández, A. (2015). Coinbase y Shift Payments lanzan la primera tarjeta de débito VISA para pagar con bitcoins en Estados Unidos. Retrieved from http://criptonoticias.com/coinbase-y-shift-payments-lanzan-la-primera-tarjeta-de-debito-visa-para-pagar-con-bitcoins/

Hernández, Á. (2015). Bitcoin en la “Milla de Oro” madrileña: ¿qué hace una moneda como tú en un barrio como este? Retrieved from http://www.eldiario.es/hojaderouter/internet/la_calle-bitcoin-serrano-milla_de_oro_0_286621458.html

Martín Fernández, J. (2015). Sobre el IVA y los bitcoins. Retrieved from http://cincodias.com/cincodias/2015/06/09/mercados/1433873155_593057.html

Merino, P. P. (2015). Ingenico y Bitpay presentan un nuevo proyecto de pago con bitcoin a través de un TPV tradicional. Retrieved from http://ecommerce-news.es/servicios/metodos-de-pago/ingenico-y-bitpay-presentan-un-nuevo-proyecto-de-pago-con-bitcoin-a-traves-de-un-tpv-tradicional-31967.html

Moratalla, M. (2015). ¿Y si los griegos se pasan al bitcoin? Ventajas y peligros de la criptodivisa. Retrieved from http://vozpopuli.com/economia-y-finanzas/64990-y-si-los-griegos-se-pasan-al-bitcoin-ventajas-y-peligros-de-la-criptodivisa

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Consulted*, 1–9. http://doi.org/10.1007/s10838-008-9062-0

Tribunal de Justicia de la Unión Europea. (2015). El cambio de divisas tradicionales por unidades de la divisa virtual «bitcoin» está exento del IVA. *Curia*.

IX. BIBLIOGRAFÍA CONSULTADA

(INTECO), I. N. (2014). *Bitcoin: Una moneda criptográfica*. Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf

BBVA. (2013). ¿Qué es Bitcoin?

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin : Economics, Technology and Governance. *American Economic Association*, 29(2), 213–238.

Brito, J. C. (2011). *Manual básico (para legisladores y diseñadores de políticas).*

Cinco Días. (Enero de 2015). Obtenido de http://cincodias.com/cincodias/2015/01/20/mercados/1421766103_969462.html

Cinco Días. (Abril de 2015). *Cinco Días*. Obtenido de http://cincodias.com/cincodias/2015/04/27/economia/1430151295_567143.html

Commons, C. (2013). *¿Qué es Bitcoin? Una sencilla introducción.*

EC. (Agosto de 2015). Dos empresas españolas se unen para crear la mayor red de cajeros de 'bitcoins'. *El Confidencial*. Obtenido de http://www.elconfidencial.com/economia/2015-08-14/dos-empresas-espanolas-se-unen-para-crear-la-mayor-red-de-cajeros-de-bitcoins_968061/

Eyal, I., & Sirer, E. G. (2015). Bitcoin-NG: A Secure, Faster, Better Blockchain. *Journal of Chemical Information and Modeling*. http://doi.org/10.1017/CBO9781107415324.004

García de la Cruz, R. (2015). *Expansión.* Obtenido de http://www.expansion.com/encuentros/rodrigo-garcia-de-la-cruz/2015/05/06/

González, J. M. (2013). *Bitcoin: La moneda del futuro: Qué es, cómo funciona y por qué cambiará el mundo.*

Mora Afonso, V. (13 de Junio de 2013). *Design and implementation of a Bitcoin Simulator.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/37001/7/vmoraafTFM0

614memoria.pdf

Móran, C. (Septiembre de 2015). ¿Dónde pago con «bitcoins» en Galicia? *La Voz de Galicia*.

Moreno, L. (s.f.). *Bitcoin: definición y características.* Obtenido de http://unimooc.com/Bitcoin-definicion-caracteristicas/

Nakamoto, S. (2013). Bitcoin: Un sistema de efectivo electrónico usuario a usuario. Introducción transacciones.

Plassaras, N. A. (2013). Regulating Digital Currencies: Bringing Bitcoin. *Chicago Journal of International Law*. Obtenido de Chicago Journal of International Law: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1407&context=cjil

Priego, M. (Septiembre de 2014). *PractiFinanza*. Obtenido de http://practifinanzas.com/2014/09/bitcoin-comercio-especulacion-en-moneda-virtual/#sthash.sayhxq4r.dpuf

Ramírez Morán, D. (2014). *Fundamento de las Divisas Virtuales: Bitcoin.*

Rampton, J. (2014). How Bitcoin Is Changing Online eCommerce. *Forbes*. Obtenido de http://www.forbes.com/sites/johnrampton/2014/07/02/how-bitcoin-is-changing-online-ecommerce/

Romero, P. (2014). Se buscan usuarios de bitcoin desesperadamente. *El Mundo*. Obtenido de http://www.elmundo.es/tecnologia/2014/11/16/546327d6268e3e9a068b4572.html

Servizio, A. &. (2009). *Bitcoin, ¿El dinero del Futuro? .*

ShenTu, Q., & Yu, J. (2015). Research on Anonymization and De-anonymization in the Bitcoin System, (1), 1–14. Retrieved from http://arxiv.org/abs/1510.07782

The Economist. (Octubre de 2015). Obtenido de http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Times, T. F. (3 de November de 2013). How will blockchain technology transform financial services? *The World Economic The World Economic*. Obtenido de https://agenda.weforum.org/2015/11/how-will-blockchain-technology-transform-financial-services/

Toledo, D. (Mayo de 2014). Destinia hace caja con el 'bitcoin' pero teme que Gobiernos y bancos lo hundan. *El Confidencial* . Obtenido de http://www.elconfidencial.com/empresas/2014-05-01/destinia-hace-caja-con-bitcoins-pero-teme-que-gobiernos-y-bancos-hundan-la-moneda_124257/

Valero Iglesias, M. (Enero de 2015). *Cinco Días*. Obtenido de http://cincodias.com/cincodias/2015/01/28/finanzas_personales/1422448142_548789.html

X. ANEXOS

Anexo 1: ¿Qué es una cartera?

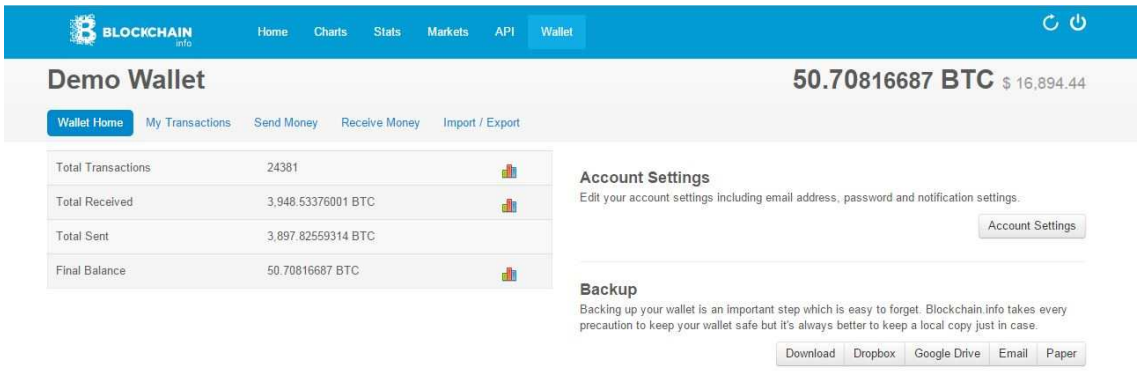


Ilustración 10: Monedero (Wallet Home)

Fuente: https://blockchain.info/es/wallet/demo-account

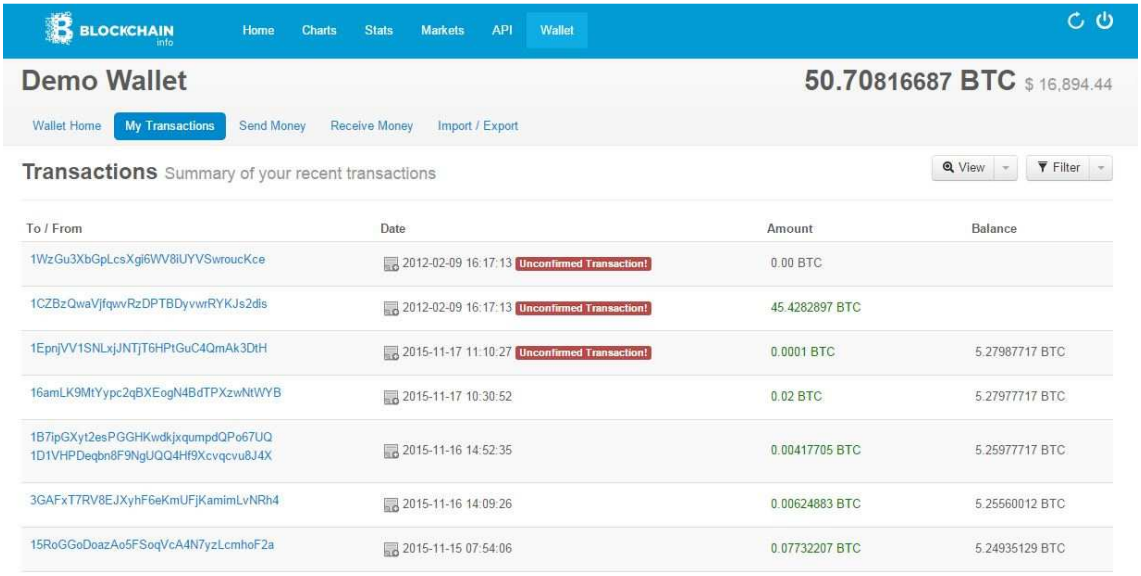


Ilustración 11: Transacciones

Fuente: https://blockchain.info/es/wallet/demo-account

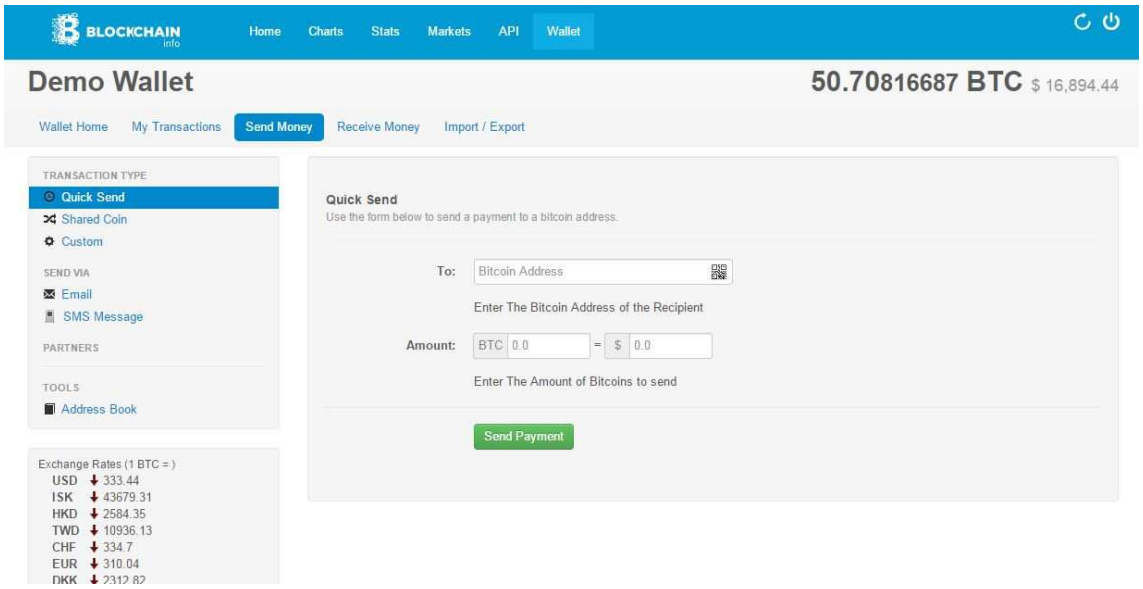


Ilustración 12: ¿Cómo enviar bitcoins?

Fuente: https://blockchain.info/es/wallet/demo-account

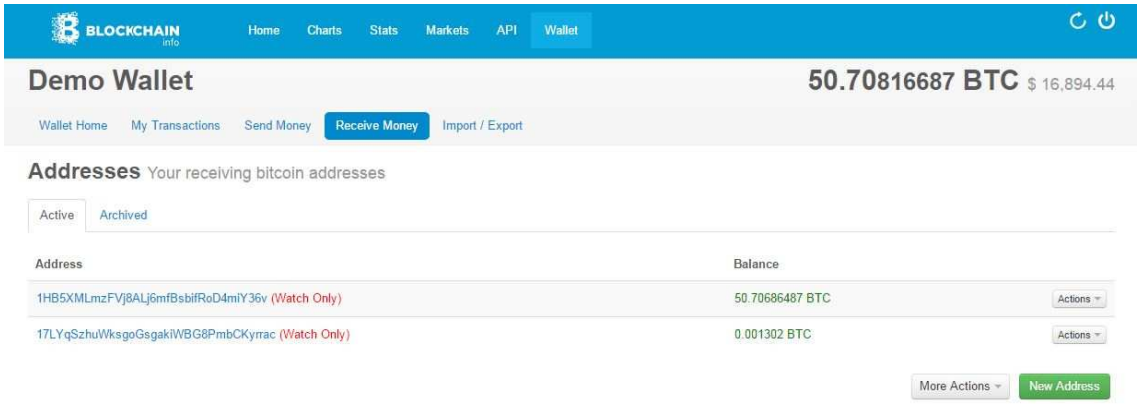


Ilustración 13: ¿Cómo se reciben los bitcoins?

Fuente: https://blockchain.info/es/wallet/demo-account

Anexo II: Listado de comercios en España que aceptan Bitcoin.

Tiendas Online

Bit2me	Obtén euros en el cajero a través de tus Bitcoins
Destinia	Ofertas en hoteles, vuelos y apartamentos - Agencia Viajes
Telepienso	Comida para animales (perros, gatos,...). Envíos a España (incl. Canarias) y Portugal.
Ogge	Tienda erótica con miles de productos y Discreción garantizada.
Zas robapinza	Bisutería, calzado, piercing, ropa y complementos.

Antarcticled	Venta iluminación LED | Bombillas LED España
Sportfans	Tienda de rugby. También disponible tienda física en Madrid.
Nexusosx86	Computers y gadgets.
Bitphone	Carga tu móvil rápido y seguro. También disponible tienda física en Alicante.
enREDados	Hospedaje web con soporte de JSP/Servlets mediante Tomcat, HTML/PHP …
Lagar la Pinilla	Lagar con vinos artesanos y aceite de oliva. También tienda física.
SpicesCaves	Comprar especias de todo el mundo, tés, rooibos y sales…
BitDomian.Biz	Registro de dominios completamente anónimos.
NESTORGAMES	Juegos de mesa ligeros y portables (físicos, no digitales). Más de 60 diferentes.
Morrotel	Proveedor VoIP (Llamadas SIP y acceso indirecto mediante números fijos y móviles).
YoUsoBitcoin.eu	Artículos publicitarios Bitcoin con la intención de popularizar su uso a través de las tiendas on-line.
Altamira21.com	Web Inmobiliaria con más de 3.000 inmuebles en Cantabria y Norte de España.
CantabriaRustica	Web especializada en la venta de inmuebles rústicos y singulares en Cantabria.
Oxcars-2011	Entradas para la cuarta edición de los Oxcars: el mayor evento de cultura libre de todos los tiempos.
Bitcoin España	Grupo de Facebook para usuarios de Bitcoin en España.
Mimetix	Diseño Web, Tiendas online, Posicionamiento y Marketing Online.
Deportes Pineda	Todo para la pesca deportiva y profesional, electrónica náutica y productos para todas las modalidades de pesca.
MaisMedia	Consultoría Web e Internet Marketing - Desarrollo y Optimización Web para ser encontrado en Internet.
SOLIGAIA	Herboristería online, dietética, cosmética natural y productos naturales seleccionados.
Elinformatico.org	Servicios profesionales informáticos en Internet, hosting, correo, desarrollos web y posicionamiento para PYMES y particulares.
SexShop21.com	Sex-shop con más de 1000 productos eróticos y envíos a toda España (inc. Canarias, Ceuta y Melilla).
Tximino Art	Tximino Art es una tienda online especializada en Art Toys, libros ilustrados, comics de autor y mucho más.
Chapas.org	Consumibles y máquinas para montar chapas.
Llaveros.biz	Modelos en plástico, piel y metal de llaveros

Andrés Morales	Diseñador gráfico. También disponible en tienda física
Holiday Apartment	Alquiler de apartamentos en Tenerife.

Madrid	Do Eat	ABC Serrano
	Ágata Ruiz de la Prada	The Geographic Club
	Dr. Emilio Santos	FJ- Martin Abogados
	La Castela	Cafetería Villalar
	Abanlex	Muñoz González Arquitectos
	Check-in Madrid	Esferared
	OneShot Hotel 04	Sportfans
	Restaurante El Tío Palomo	OnlyUsa

Barcelona	Vaciados Barcelona
	Restaurante Osgalegos
	Nicstudios
	Soligaia
	Nostrum Aribau
	ONG - Sonríe y Crece
	Yoigo en Barcelona
	The Dog is Hot
	Chupacabras3D

Comunidad Valenciana	**Valencia**
	Acquamatter
	Clínica dental Carralero
	Alicante
	Bitphone.es

Andalucía	Casa Rural en Sevilla
	Minaca Inmobiliaria

Galicia	SERED.NET

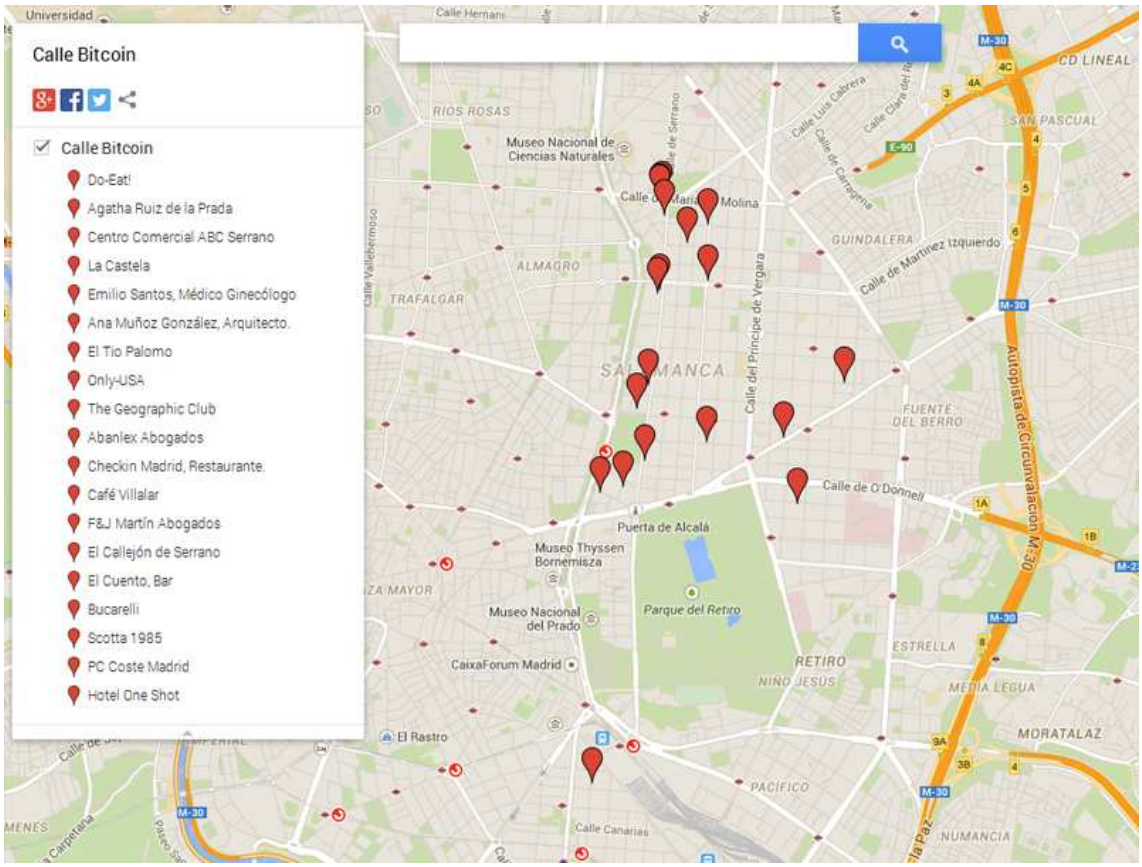
Valladolid	DYM Peluqueros

Salamanca	1000tel.com

Baleares	Cafetería Cent Deu

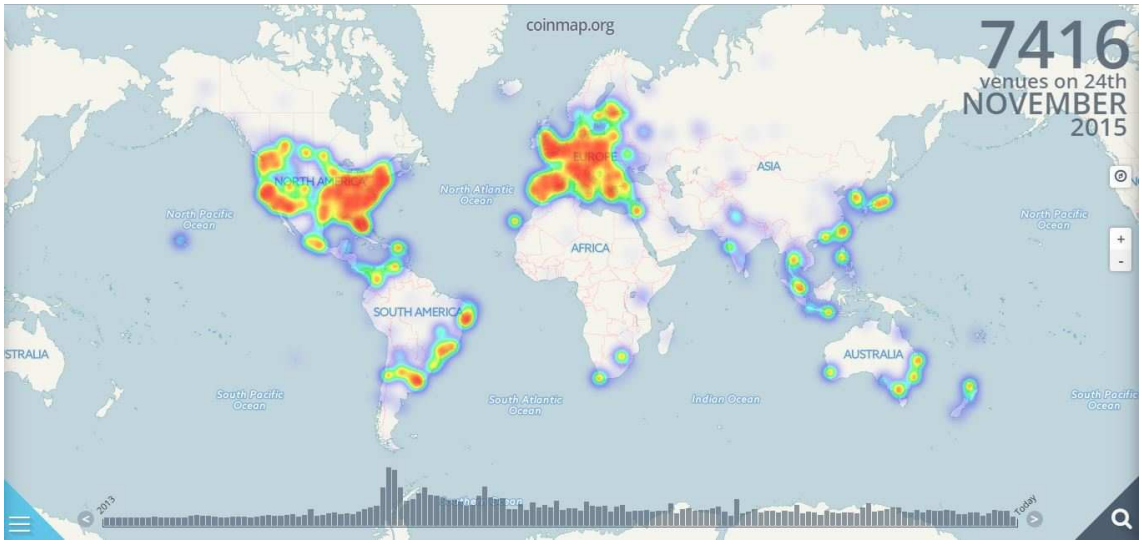
Tabla 1: Lista de Comercio en España con Bitcoin

Anexo III: Calle Bitcoin



Fuente: http://www.expansion.com/

Anexo IV: Mapa de calor Bitcoin



Fuente: http://www.coinmap.org