

MEMORIA DEL TRABAJO FIN DE GRADO

Evolución y aplicación de las criptomonedas como método de pago.

Application and evolution about cryptocurrencies as medium of exchange.

Autor: D. Óscar Ibarria Morera

Tutor: D. Francisco J. Ledesma Rodríguez .
Departamento de Economía Contabilidad y Finanzas.

Grado en ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS
FACULTAD ECONOMÍA EMPRESA Y TURISMO
Curso Académico 2018/2019

En San Cristóbal de La Laguna a 9 de Septiembre de 2019.

“ Nunca invierta en negocios que usted no pueda entender”
Warren Buffet.

TÍTULO: Evolución y aplicación de Criptomonedas como método de pago.

AUTOR: Oscar Ibarria Morera

TUTOR: Francisco J. Ledesma Rodríguez.

DEPARTAMENTO: Economía, Contabilidad y Finanzas.

RESUMEN

Mediante la elaboración de este TFG abordaremos la evolución de manera general y sencilla de las criptomonedas. Para ello se explicará la creación de estas, deteniendonos en las principales criptomonedas actuales con mayor detenimiento y el sistema Blockchain en el que se sustentan, implantación, seguridad y estabilidad.

También se detallaran aspectos como tipo actual de usuarios, su evolución en el tiempo y la presencia en diferentes países. Siendo la finalidad la aplicación en la vida cotidiana y la revolución que pueden aportar a el mundo su utilización como medio de pago.

PALABRAS CLAVE:

Bitcoin, criptomonedas; blockchain; medio de pago.

ABSTRACT:

Through the development about this TFG we will address the evolution in a general and simple way of cryptocurrencies. This will explain the creation of these, stopping in the main current cryptocurrencies with greater detail and the Blockchain system on which they are based, implementation, security and stability.

Aspects such as current type of users, their evolution over time and presence in different countries will also be detailed. The purpose being the application in everyday life and the revolution that can contribute to the world its use as medium of exchange.

KEYWORDS:

Bitcoin, Cryptocurrencies, Blockchain, medium of exchange.

ÍNDICE CONTENIDO

1. INTRODUCCIÓN.....	6
2.MARCO CONCEPTUAL.....	7
2.1.CONCEPTO Y FUNCIONES DEL DINERO.....	7
2.2 DINERO REAL EN CIRCULACIÓN.....	9
2.3 COMPARACIÓN ENTRE MONEDAS DE CURSO LEGAL Y CRIPTOMONEDAS	13
2.4 DIFERENCIA ENTRE CRIPTOMONEDAS Y DINERO ELECTRÓNICO O DIGITAL.....	15
2.5 DESARROLLO DE LAS CRIPTOMONEDAS: BLOCKCHAIN.....	15
3. CRIPTOGRAFÍA , CREADOR(ES), BLOCKCHAIN, SISTEMA MINER Y PERFIL USUARIOS.....	16
3.1 ¿QUÉ ES LA CRIPTOGRAFÍA?.....	16
3.2 ¿POR QUÉ FUERON CREADAS Y QUIÉN LAS CREÓ?.....	17
3.3 ¿EN QUÉ SISTEMA SE BASA BLOCKCHAIN?	
3.4 ¿CÓMO SE GENERAN? SISTEMA MINER.....	19
3.5 PERFILES DE USUARIOS.....	22
4. METODOLOGÍA.....	22
4.1 BITCOIN COMO MÉTODO DE PAGO.....	22
4.2 COMPARACIÓN PRINCIPALES MÉTODOS DE PAGO.....	22
4.3 INVESTIGACIÓN COMO MÉTODO DE PAGO EN WEB OF SCIENCE.....	24
5. CONCLUSIONES	26
6. BIBLIOGRAFÍA.....	27
CONSULTADOS EN WOS.....	29

ÍNDICE DE TABLAS Y FIGURAS

Figura 1. Oro repartido a nivel Mundial.....	10
Figura 2. Se presenta su reparto por países y regiones.....	11
Tabla 2.1 Dinero fiduciario y Bitcoin.....	12,13
Figura 3. Diagrama funcionamiento Blockchain (sistema de bloques).....	15
Figura 4. Funcionamiento economía Bitcoin basada en Blockchain.....	18
Figura 5. Monedero electrónico Coinbase.....	19

1. INTRODUCCIÓN

Un nuevo tipo de dinero, sustitutivo al dinero fiduciario. Está entre otras era una de las pretensiones más significativas del Bitcoin, cuando salió a la luz en 2007.

El objetivo principal de este trabajo de Fin de Grado consiste en observar la evolución que han sufrido las criptomonedas desde su inicio en 2007, destacando su papel de transformarse dependiendo los intereses de sus usuarios hasta la actualidad.

En un primer momento surgieron como una alternativa al dinero fiduciario, para utilizarse como medio de pago. Esta función del dinero pasó a un segundo plano, retomando en un último momento, ya que se ha sido utilizado por inversionistas con carácter especulador.

Desde su creación a través del Bitcoin, en el mercado ha aparecido una gran diversificación de este tipo de monedas, las cuales poseen diversidad de ventajas y facilidades de uso según interesen a sus usuarios.

La metodología seguida se ha realizado explicando de manera teórica una aproximación a las formas y tipos de dinero existente, en que se basa y sus cualidades. Seguidamente se procederá a una comparación de las ventajas e inconvenientes del dinero fiduciario frente al Bitcoin, para terminar de manera teórica examinando el sistema en el que se basa esta criptomoneda a través de su historia y síntesis de su funcionamiento. Para realizar un análisis más exhaustivo se acotará hacia la criptomoneda predominante; el Bitcoin. Tras esto se procederá a realizar un exhaustivo análisis de la literatura acerca de la utilización de Bitcoin como método de pago, citando los respectivos estudios actuales en este área, desvelando así sus limitaciones desde diferentes vertientes. Examinando su uso como método de pago, si se ha incrementado o disminuido desde su creación y comprobar si podría realmente sustituir al dinero fiduciario.

2.MARCO CONCEPTUAL

2.1.CONCEPTO Y FUNCIONES DEL DINERO

El Banco Central Europeo (2015) presenta la naturaleza del dinero a través de su evolución a lo largo del tiempo. En su creación era un objeto hecho de un material con valor de mercado, como las monedas de oro, denominado dinero mercancía. Tras este surgió el dinero representativo, que consistía en billetes que podían cambiarse por una determinada cantidad de oro y plata. En la actualidad, en las economías modernas, entre las que se encuentra la zona euro, se utiliza el dinero fiduciario, declarado de curso legal y emitido por los respectivos bancos centrales. El BCE enfatiza en su valor intrínseco, siendo aceptado por los ciudadanos a cambio de bienes y servicios, ya que confían en que el banco central mantenga estable el valor de la moneda y su perdurabilidad a lo largo del tiempo.

Siguiendo a Mankiw (2009), Krugman o Wells (2007) las funciones del dinero son principalmente tres, actuando como: (1) medio de pago o cambio, (2) depósito de valor y (3) unidad de cuenta. A través de dichas funciones se diferencia el dinero de otros activos económicos como bonos o acciones. Nos centraremos en las funciones del dinero como depósito de valor y medio de pago, profundizando así en el concepto de dinero y el sistema de confianza en el que se sustenta.

1 Como medio de pago:

Es la función primordial del dinero, facilitar el intercambio por tratarse de un bien convencional de aceptación general y garantizada. Consiste en el uso del dinero para realizar cualquier tipo de transacción, facilitando así el intercambio de bienes y servicios. Como indica Solano (2007) esta función trata de "inculcar que se recibe una cosa a cambio de otra".

2 Como depósito de valor:

Esta función consiste en que el dinero es una forma de riqueza para poder comprar algo en un futuro. El dinero tiene la capacidad de mantenerse estable a lo largo del tiempo.

3 Unidad de cuenta:

El dinero permite determinar las unidades de valor, o los precios que tienen los bienes, productos y servicios. Esta función del dinero, facilita hacer los cálculos económicos, fraccionar el dinero y saber cuanto cuesta cada una de las cosas que deseamos adquirir. Permite otorgar un precio para poder comercializar.

Formas del dinero:

Tal y como indica Castillo (2018) en su artículo para la "EAE Harvard School", es posible identificar diferentes tipos de dinero. Desde su origen hasta la actualidad y teniendo en cuenta la cantidad de cambios sociales, económicos y políticos que se han presentado desde la civilización griega hasta nuestros días, el dinero sigue conservando prácticamente la misma función: servir de herramienta como intercambio comercial de valor entre los individuos que lo consideren como tal. Así, es posible destacar en la actualidad los siguientes tipos de dinero:

1. Dinero fiduciario:

Es el dinero que utilizamos cotidianamente. Su valor, no está en los billetes o monedas ni en el papel o metales del que está compuesto este. Representa el valor por alguna autoridad financiera en ciertos mercados o lugares para ello, todo sustentando por el *sistema de confianza*. El dinero fiduciario, es el resultado de un pacto social respetado por todos sus usuarios.

2. Dinero de mercancía:

Dinero con un valor en sí mismo que representa un valor establecido. No es una representación arbitraria de un valor, a diferencia del dinero fiduciario, sino que hay una equivalencia exacta entre lo que vale y lo que representa en un contexto determinado, los ejemplos más claros del dinero mercancía son las monedas de oro y la plata.

3. Dinero legal:

Más que un formato, se trata de una denominación que engloba todas aquellas monedas emitidas por una entidad o ente facultado, bancos centrales, bancos federales o casas de la moneda de determinados países. El dinero legal es aceptado por todos los miembros de una comunidad y además, que posea respaldo de autoridades.

4. Dinero bancario:

Originado por entidades bancarias, engloba todos los depósitos bancarios mantenidos por parte de la clientela. El dinero bancario actualmente está formado por los depósitos a la vista existentes en las entidades de depósito y, en un sentido más amplio, se incluye también el crédito disponible a la vista por los clientes del sistema bancario.

5. Dinero pagaré:

Es un documento contable que contiene la promesa incondicional de una persona, denominada suscriptora (o deudor) que pagara a una segunda persona , denominada beneficiario (o acreedor) una suma determinada de dinero en un determinado plazo de tiempo.

Es una declaración de obligaciones. Se emite al portador y surge de las palabras ``debo y pagaré``.

Continuando con Castillo (2018) es preciso destacar un nuevo tipo de dinero, dentro de las formas ya existentes y que es debido al grado de digitalización y el desarrollo de nuevas tecnologías que ha propiciado un nuevo cambio de formato y adquiera características que hasta el momento no había tenido.

6. Dinero electrónico:

También llamado dinero digital, es aquel que no existe de manera física, es decir en papel moneda tradicional, pero que posee las mismas funciones de intercambio de valor, produciéndose estas transacciones a través de redes como internet u otros medios de carácter electrónico. En los últimos años se ha apreciado un auge de este tipo de dinero, que supone enormes ventajas como el ahorro de tiempo, recursos y sobre todo, la superación de barreras geográficas. En este tipo se incluyen las criptomonedas, aunque estas no posean una regulación ya que no son emitidas por ningún ente de control regulatorio.

2.2 DINERO REAL EN CIRCULACIÓN

2.2.1 Agregados Monetarios

Siguiendo, por ejemplo, a Cabezas (2018) los Agregados Monetarios son agrupaciones de diferentes tipos de dinero, según la liquidez de los activos que incluyen. Para construir los Agregados Monetarios es necesario seleccionar qué instrumentos financieros se consideran dinero, es decir, establecer lo que se denomina instrumentos financieros. Estos instrumentos se pueden evaluar en función de: su **liquidez** (capacidad para ser fácilmente transformados en dinero) y de su **confiabilidad** (del grado razonable de certeza sobre su valor presente y futuro).

Los bancos centrales tienen varias medidas de la masa monetaria, identificándose con la letra M (Money en inglés) seguida de distintos números, que expresan una definición de dinero cada vez más amplia y menos líquida. Tanto el Banco Central Europeo (BCE) como el Banco de España fijan como agregados a M1, M2 y M3, siendo este último, el agregado monetario más estable y,

por ello, ha sido elegido por el Eurosistema dentro de su estrategia de política monetaria, para definir un valor de referencia para el crecimiento económico.

El BCE presenta las siguientes definiciones de estos:

- *Narrow money (M1)*, incluye la moneda, billetes y monedas, así como los saldos que pueden convertirse inmediatamente en moneda o utilizarse para pagos sin efectivo, es decir, depósitos a la vista.

M1= Efectivo en manos del público (efectivo en circulación monedas y billetes)+ depósitos a la vista.

- *Intermediate money (M2)* comprende el dinero limitado(M1), añadiendo los depósitos con un vencimiento de hasta dos años y los depósitos canjeables en un período de preaviso de hasta tres meses. Dependiendo de su grado de liquidez, estos depósitos pueden convertirse en componentes de M1. M2 refleja el interés particular en analizar y monitorear un agregado monetario que, además de la moneda, consiste en depósitos que son líquidos.

M2=Compuesto por los pasivos incluidos en M1+ Depósitos a plazo de hasta dos años + Depósitos disponibles con preaviso de hasta tres meses.


- *Broad money (M3)*, comprende M2 en instrumentos negociables emitidos por el sector de las *IMF*. En este agregado se incluyen ciertos instrumentos del mercado, en particular acciones/unidades del fondo del mercado monetario y los acuerdos de recompra. Se caracterizan por un alto grado de liquidez y certeza de precios hace que estos instrumentos sean sustitutos cercanos de los depósitos. Como resultado de su inclusión, M3 se ve menos afectado por la sustitución entre varias categorías de activos líquidos(M1), lo que le confiere ser el agregado monetario más estable, por ello ha sido elegido por el Eurosistema, dentro de su estrategia de política monetaria como un valor de referencia para el crecimiento del dinero.

M3= Pasivos incluidos en M2 + Cesiones temporales + Participaciones en fondos del mercado monetario + Valores de renta fija de hasta dos años emitidos por instituciones financieras monetarias.

La forma que utiliza el BCE para medir estos agregados monetarios es a través del balance consolidado de aquellas Instituciones Financieras Monetarias (IFM) residentes en el área euro y que son las emisoras de dinero.

2.2.2 Algunos datos relevantes

A continuación se presenta de manera gráfica la cuantificación actual y más reciente de la masa monetaria total a nivel mundial, disponible en el artículo ``All of the world's Money and Markets in One Visualización'' de Desjardins(2017). worlds-money-markets-one-visualization-2017

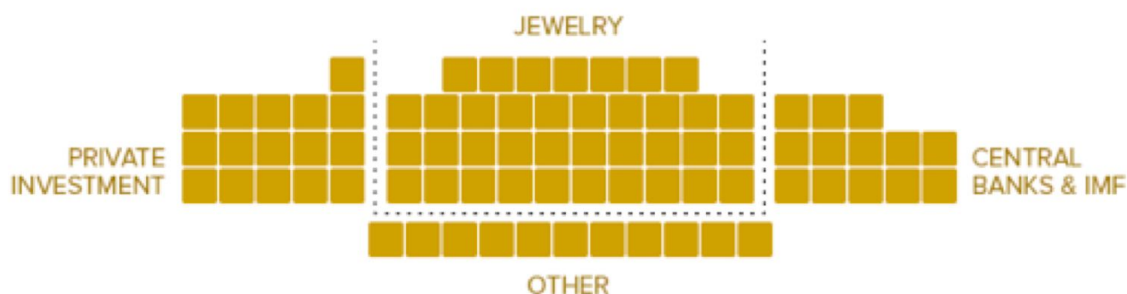

 Este recuadro representa 100 billones de \$; lo tomaremos como guía de referencia.

- Plata:** el valor del conjunto de plata mundial está valorado en 17 billones de \$, perteneciendo esta a mercados de capitales.

Valor de la Plata : 

- Valor del oro:** Valorado en 7.7 trillones y repartido de manera tanto pública como privada. El oro siempre se ha considerado un depósito de valor.

Figura 1. Oro repartido a nivel Mundial.



Fuente: <http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/>

- Ø **Private Investment:** Oro que se encuentra en inversiones privadas.
- Ø **Jewelry:** Joyerías a nivel mundial.
- Ø **Central Banks & IMF:** Es el oro almacenado en reservas con el que se respaldan las instituciones financieras monetarias (*IMF*) a nivel mundial para acreditar de valor a sus billetes y monedas.
- Ø **Other:** Oro repartido a nivel mundial en utensilios, piezas de museos, etc.

Siguiendo a Criptotario (2018) en 1995 surgió la plataforma E-Gold, que fue la primera moneda digital respaldada enteramente por el oro, en su apogeo fue muy utilizada hasta que finalmente el servicio fue dado de baja. Hubo otros intentos para crear este tipo de moneda virtual, pero

todos anteriores a Bitcoin y la tecnología Blockchain. En la actualidad encontramos distintos tipos de criptomonedas respaldadas por oro. También páginas entre las que destacan Vaultoro, en la que se puede comprar oro en segundos si posees Bitcoins, encontrándose este oro en bóvedas Suizas. Bankia (2016) sugiere la utilización de las criptomonedas como método pago, ya que este es un modelo económico nuevo, que no tardará en implementarse. La civilización humana se ha adaptado a los modelos económicos, entre ellos el patrón oro y su cambio a dinero fiduciario.

Continuando con Desjardins (2017), encontramos las criptomonedas.

- **Criptomonedas:** El activo que está creciendo a mayor velocidad son las criptomonedas; sin duda en muy poco tiempo están incrementando su valor en el mercado mundial. En 2017 llegaban a una capitalización de 100 billones de \$.

Bitcoin: \$100 billones.

Ethereum: \$28 billones.

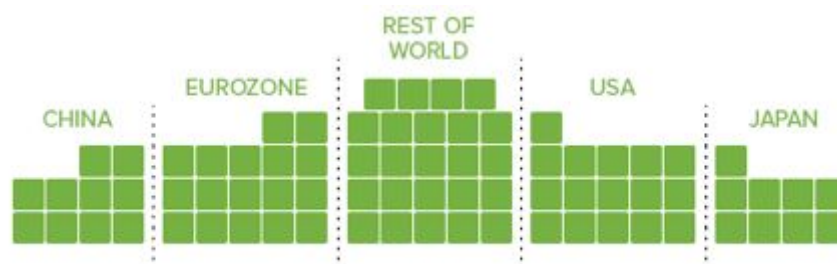
Resto de criptomonedas: \$45 bill.



Bit2me (2018) presenta la evolución de Bitcoin. Esta criptomoneda se puso inicialmente en el mercado con un precio de cero y dos años más tarde era utilizado a modo de prueba por intercambio entre fans. En 2010 se realizó la primera compra utilizando Bitcoins, con el que se compraron 2 pizzas en Jacksonville, Florida por 10.000 BTC (1 BTC=0.003\$). Lentamente empezó a valorizarse debido a la entrada de usuarios al sistema y que utilizaban esta criptomoneda como método de pago, alcanzando su máximo histórico en diciembre de 2017 en el que 1 BTC llegó a la cifra de 21.000\$.

- **Monedas(dinero líquido):** El dinero mundial en circulación supone \$7.6 trillones. Repartido entre estos países. Lo que supone un 8% de la masa monetaria total.

Figura 2. Se presenta su reparto por países y regiones.



Fuente: [worlds-money-markets-one-visualization-2017](https://www.worlds-money-markets-one-visualization-2017)

Para finalizar con Desjardins (2017) encontramos los stock markets (mercados de valores). Estos mercados alcanzan una capitalización a nivel mundial de unos 73 trillones de dólares. Aunque los mercados de derivados financieros poseen la mayor masa monetaria, esto es debido a su carácter especulativo y donde sólo un 1% de las operaciones se realizan en la fecha pactada por sus usuarios, con 544 trillones de dólares. Antes de la gran crisis mundial, estos mercados de derivados ascendían a 1,2 cuadrillones de \$, lo cual podría evidenciar la alta especulación de estos mercados.

2.3 COMPARACIÓN ENTRE MONEDAS DE CURSO LEGAL Y CRIPTOMONEDAS

Siguiendo a Díaz (2018) ``debemos tener claro que Bitcoin funciona de forma similar al dinero fiduciario, tomando en cuenta que éste se define como activo o bien generalmente aceptado como medio de pago por las partes involucradas en un intercambio económico''. En cambio el dinero fiduciario constituye la moneda de curso legal de cada país, encontrándose respaldado por entidades económicas legítimas. Tiene una representación física y/o electrónica y cada banco central, mediante el uso de determinadas políticas controla cuánto dinero circula en su economía. Por su parte, las criptomonedas, no poseen la categoría de ``moneda de curso legal'' en ningún país, ni están respaldadas por un gobierno o Banco Central.

Tabla 2.1 Dinero fiduciario y Bitcoin.

DINERO FIDUCIARIO	BITCOIN
CARACTERÍSTICAS	
Medio físico y/o digital de intercambio	Medio de intercambio totalmente digital.
Representado por billetes y monedas, o dinero electrónico	Representado por registros únicos respaldados por una red tecnológica
Suministro ilimitado. Las entidades designadas emiten tanto dinero como se necesite	Suministro limitado. Tiene un límite máximo de emisión. En el caso del Bitcoin son 21 millones.
Centralizado. Emitido y controlado por instituciones y bancos.	Descentralizado. No están controladas por ningún gobierno o entidad.

PROCEDENCIA	
Cada país tiene su propia casa de moneda, controlada por la supervisión gubernamental.	De la minería de criptomonedas, proceso informático donde computadoras especializadas buscan la solución de rompecabezas criptográficos y al resolverlo reciben una recompensa.
EN LO ECONÓMICO	
Su valor está determinado por el mercado, las regulaciones y la confianza del país emisor. La cotización del dinero aumenta o disminuye en relación con otras monedas debido a factores macroeconómicos.	Su valor está determinado por la oferta y la demanda
Su valor se ve afectado por la presión inflacionaria.	Son inflacionarias con una tasa decreciente, hasta que sean emitidas todas sus unidades.

Fuente: Elaboración propia siguiendo a

<https://www.criptonoticias.com/educacion/aprende-diferencias-bitcoin-dinero-fiduciario/>

En la Tabla 2.1 podemos observar que las principales diferencias radican en legitimidad, procedencia u origen. Como afirma Nieto(2018), las criptomonedas son descentralizadas y se crean a través de *miners*, **mientras que el dinero fiduciario es emitido y controlado por instituciones financieras**. En alusión a la inflación seguimos a Herrera (2018), quien indica que se conoce por *Bitcoin Halving* a la declaración en el código *Bitcoin* que reduce la recompensa de los mineros a la mitad y que ocurre cada cuatro años. En un primer momento la recompensa era de 50 BTC cada 10 minutos (tiempo en el que se añade un bloque de un minero específico, a la cadena *Blockchain*) y actualmente después de los dos últimos cortes es de 12.5 BTC. Uno de los propósitos en la creación *Bitcoin*, era establecer un sistema autosostenible, en el que su creador Nakamoto, se inspiró en la extracción de oro para implementar la minería de criptomoneda, fijando el límite en 21 millones de *Bitcoins*. Se estima que el último Bitcoin obtenido como recompensa por los *miners*, será en 2140.

2.4 DIFERENCIA ENTRE CRIPTOMONEDAS Y DINERO ELECTRÓNICO O DIGITAL

Descentralización y criptografía

Tomando como referencia al Banco de España, en su Glosario General, es dinero electrónico todo aquel “sustitutivo electrónico de las monedas y los billetes de banco, almacenado en un soporte electrónico como, por ejemplo, una tarjeta inteligente y que, en general, está pensado para efectuar pagos electrónicos de cuantía limitada”.

Las peculiaridades de este dinero podemos encontrarlas en el BOE: Ley 21/2011, de 26 de Julio, de dinero electrónico. Publicado en «BOE» núm. 179, de 27 de Julio de 2011, páginas 84235 a 84254(20 págs). En sus diferentes preámbulos encontramos cuestiones concernientes a su regulación con las entidades a las que se encuentra adherido. A su vez estas entidades deben estar autorizadas por el Ministerio de Economía y Hacienda, de modo que “habrá que acreditar aspectos que proporcionen garantías de que la entidad va a estar sometida a una gestión sana y prudente”(BOE NÚM. 179 , miércoles 27 de Julio de 2011, SEC.1. pág.84237).

Esta es una de las diferencias con mayor peso respecto a las criptomonedas, ya que las criptodivisas a pesar de encontrarse dentro del dinero virtual, que a su vez es dinero electrónico no posee una entidad reguladora de ningún Organismo Oficial. Al no tener un Organismo Oficial de respaldo, este tipo de dinero electrónico carece de regulación. Las criptomonedas son un tipo de moneda virtual que **no tiene un único emisor ni un administrador centralizado**, por ello carece de valor intrínseco y de respaldo.

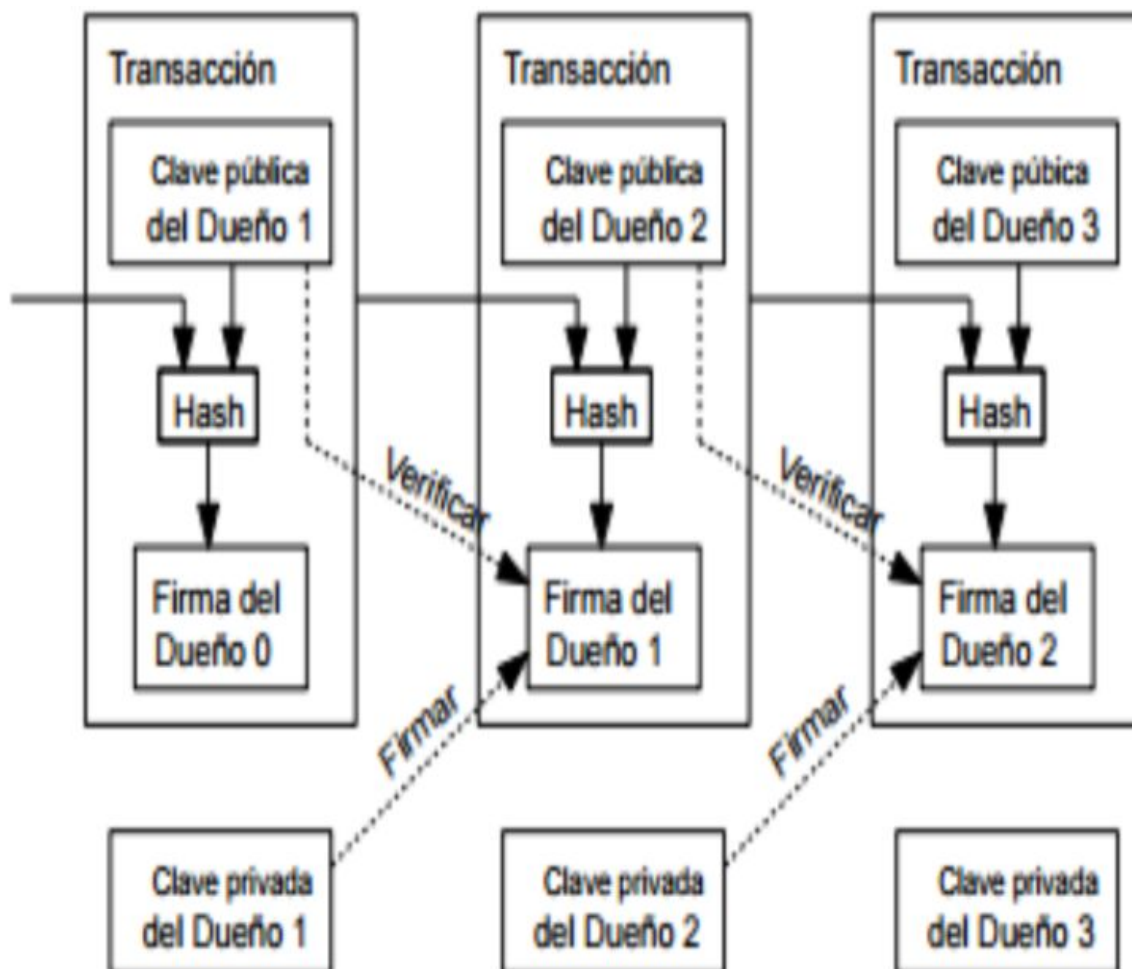
Siguiendo a Nieto (2018) es muy difícil rastrear su origen, y esto es debido a su modelo de creación y el sistema *Blockchain* en el que se sustentan. Las criptomonedas, como su nombre indica están protegidas por criptografía, es decir, se encuentran cifradas por algoritmos matemáticos, denominados *hash*, brindando así seguridad en las transacciones. También utilizan un sistema de bloques, compuesto de nodos, que es un registro de contabilidad público, el cual garantiza que cada transacción realizada sea legítima y carezca de fraude.

2.5 DESARROLLO DE LAS CRIPTOMONEDAS: BLOCKCHAIN.

El *Blockchain* funciona como un libro contable, donde la información se registra en una serie de direcciones públicas en internet, similar a una cuenta corriente, donde el número de esa cuenta lo puede conocer cualquiera(cuenta con una dirección pública y otra de carácter privado). Si el dueño de la cuenta realiza un pago, se registra en esa cuenta un debe, y por tanto debe existir otra cuenta de otra persona donde se registrará un haber. Este proceso, tal y como explica

Rosembuj (2015), se fundamenta en dos elementos: la seguridad generada mediante métodos criptográficos, y un sistema descentralizado de confirmación de transacciones, denominado blockchain.

Figura 3. Diagrama funcionamiento Blockchain (sistema de bloques).



Fuente: Elaboración propia siguiendo a [claves-tecnologicas-para-entender-el-bitcoin](#).

3. CRIPTOGRAFÍA , CREADOR(ES), BLOCKCHAIN, SISTEMA MINER Y PERFIL USUARIOS

3.1 ¿QUÉ ES LA CRIPTOGRAFÍA?

La criptografía, como explica Rosembuj (2015), es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados. Es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. En su origen , su único objetivo era

proteger la confidencialidad de informaciones militares y políticas. Las criptomonedas utilizan este mecanismo para asegurar la confidencialidad de unos determinados datos.

Siguiendo con Criptolog(2018) la criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones. Todas las criptomonedas utilizan sistemas de cifrado que las hacen virtualmente infalsificables, verificando dos pasos:

1. Se asegura que el Bitcoin enviado es legítimo y pertenece a quien lo transmite.
2. El Bitcoin solo puede ser usado por la persona que posee la clave privada de la dirección a la que se envió.

Este proceso cuenta con claves públicas y privadas, la clave pública, que es la dirección del monedero, sólo puede ser utilizada para recibir Bitcoins. La clave privada del transmisor es utilizada para firmar la transacción, asegurando que esa dirección le pertenece. Todo esto es sintetizado por los monederos y los *software* especiales en los que se sustentan. Resumiendo, esta operativa para el usuario es poner la dirección Bitcoin (clave pública) a donde se quiere enviar el dinero, añadir la cantidad y pulsar el botón "enviar".

Siguiendo con Rosembuj (2015) el objetivo es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto, las propiedades de las que se ocupa la criptografía son: confidencialidad, integridad y autenticación.

Como explica Delgado y Palacio (2006), los *hashes* criptográficos modernos, son una versión mucho más segura y compleja de esto. En general estas funciones se usan para verificar la integridad de la información, ya sea para detectar errores o intentos malintencionados de grupos de usuarios.

3.2 ¿POR QUÉ FUERON CREADAS Y QUIÉN LAS CREÓ?

En la página oficial de *Bitcoin* es posible encontrar información sobre su utilización como medio de pago por internet y, además, se considera como una moneda virtual que usa algoritmos criptográficos, un protocolo y un *software*. La conjunción de estos componentes permite la realización de transacciones casi instantáneas entre pares (*peer-to-peer* P2P) y, por consiguiente, pagos en todo el mundo con unos costes de procesado de dichas transacciones muy reducidos, o incluso nulos.

La primera aparición del Bitcoin se produjo el 1 de Noviembre de 2008, en la lista criptográfica de metzdowd.com, donde un usuario con el pseudónimo de *Satoshi Nakamoto*, había estado trabajando en un nuevo sistema de dinero electrónico. Resumiendo sus propiedades y el contenido original que describía su trabajo, mostrándose este protocolo *Bitcoin* y su *software* de referencia, "Bitcoin Core". Siguiendo con Nakamoto (2008). "He estado trabajando en un nuevo

sistema de pago electrónico que es totalmente peer-to-peer, sin una tercera parte que sirva de garante”.

Nakamoto (2008) continuaba con las propiedades:

- La falsificación se evita con una red *peer-to-peer*.
- No hay una tercera parte garante.
- Los participantes pueden ser anónimos.
- Las nuevas monedas se crean mediante un sistema denominado “prueba-del-trabajo”.

La “prueba de trabajo” para la creación de nuevas monedas también potencia la red para evitar la falsificación de la moneda. El 11 de febrero de 2009, un perfil creado en el portal P2P foundation, precisamente con el nombre de *Satoshi Nakamoto*, publicó lo siguiente: “*Bitcoin open source implementacion of P2P currency*”. En el texto, Nakamoto (2009) daba a conocer el portal oficial de *Bitcoin*, las características fundamentales de éste, el artículo donde se mostraba el diseño, e incluso, el cliente inicial con el que comenzar a participar en la red. Por el momento la identidad del creador, o grupo de creadores, no ha sido revelada, esto con el objetivo de proteger a la red *Bitcoin* y a ellos mismos. Lo único que se sabe de Satoshi Nakamoto son los datos publicados en su perfil de portal P2Pfoundation: hombre de nacionalidad japonesa de 38 años de edad (2009). Su presunción de ser un pseudónimo es debido a los conocimientos en criptografía y algoritmos matemáticos que necesitaba para crear esta red, de aquí que también podría ser un grupo de personas.

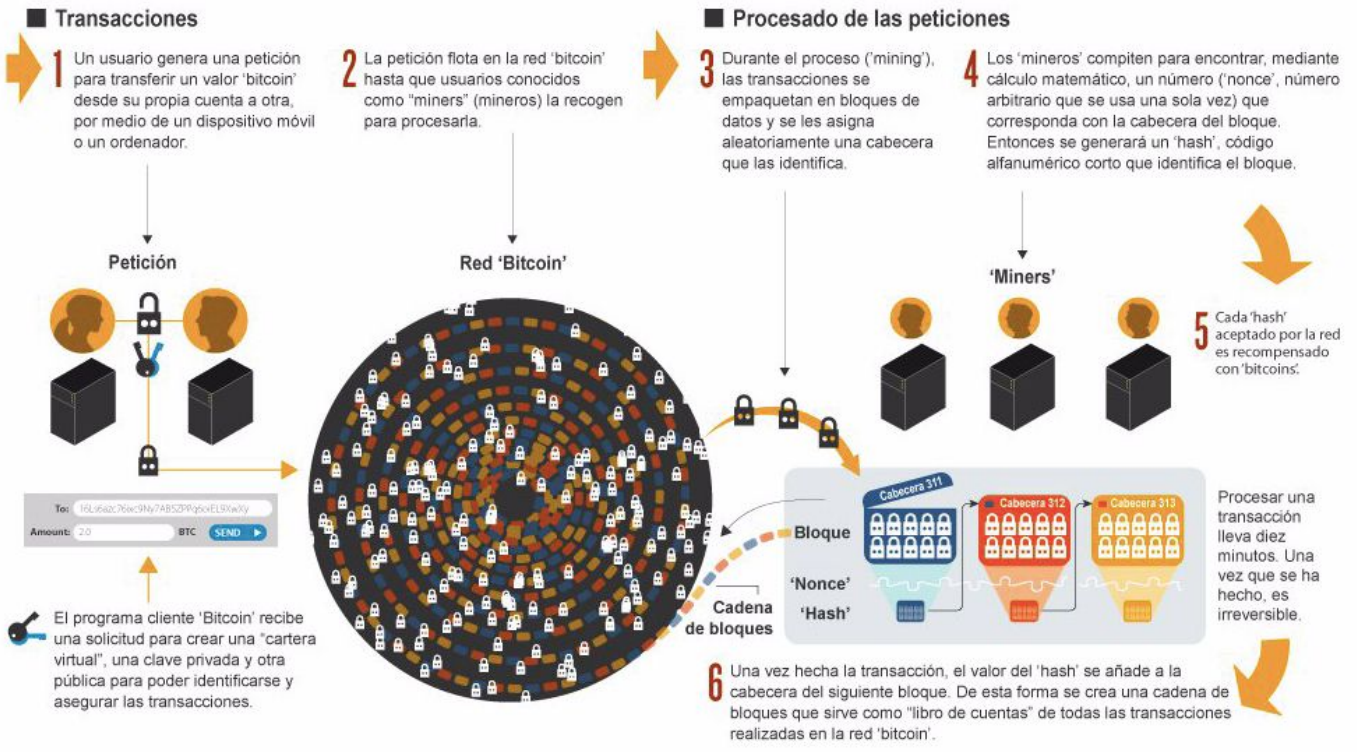
3.3 ¿EN QUÉ SISTEMA SE BASA BLOCKCHAIN?

Además de la criptografía, la mecánica del *Bitcoin* se fundamenta también en la tecnología del *Blockchain*. Siguiendo a Márquez (2016), el usuario en un primer momento elige “un monedero”, que es un programa informático, instalándolo en su ordenador o en su dispositivo electrónico (móvil o *Tablet*); cada monedero posee una llave especial creada con algoritmos de criptografía, empleadas para realizar firmas digitales y que garantizan la identidad del usuario. Tras esto se origina una dirección *Bitcoin* y esta es utilizada para transferir *Bitcoins* a otros usuarios o realizar pagos. A continuación, las transferencias se verifican por medio de un registro de contabilidad público, al alcance de cualquier usuario, denominado “*blockchain*” (cadena de bloques), que muestra todas las operaciones realizadas y confirmadas, asegurando al usuario que posee la cantidad de *Bitcoins* que pretende gastar. Cada equipo informático que participa en la red es lo que se conoce como “nodo”. No hay un servidor, no hay un servicio centralizado, y no hay una jerarquía dentro de la red.

Figura 4: Funcionamiento economía Bitcoin basada en Blockchain

Fuente: [bitcoin](http://bitcoin.com).

Cómo funciona la economía 'Bitcoin'



Según Antonopoulos (2014), la red *Bitcoin* implica, por tanto, una red de ordenadores en todo el mundo que constantemente retransmite nuevas transacciones entre sí. Cada ordenador en esta red es un nodo que tiene descargado *Blockchain*. Cualquier usuario puede ser un nodo en la red *Bitcoin*, basta con instalar el *software Bitcoin Core*. Una vez finalizada la instalación eres un nodo más dentro de la red *Bitcoin*. Continuando con Vega (2018) la cadena de bloques de bitcoin contiene un registro certero y verificable de todas las transacciones que se han hecho en su historia. Esta historia completa de transacciones se lleva en un libro registro inmutable denominado *ledger*.

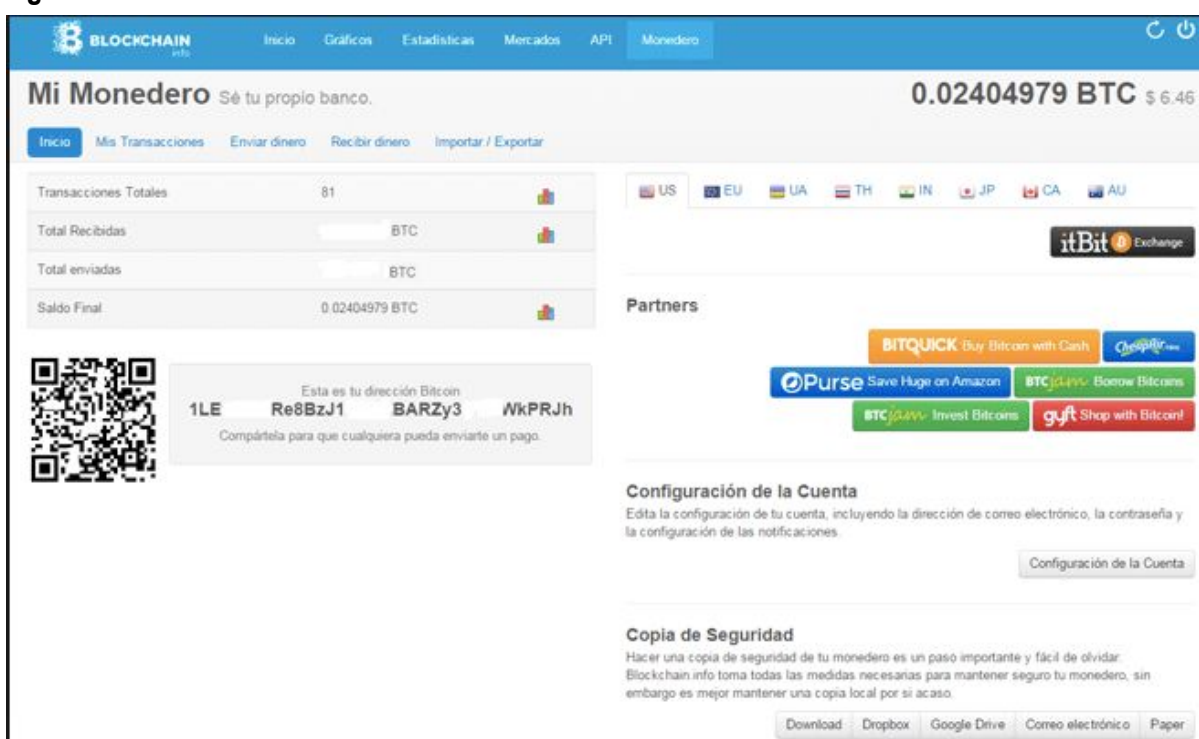
3.4 ¿CÓMO SE GENERAN? SISTEMA MINER.

Existen dos formas para obtener criptomonedas. Una de ellas es mediante la realización de transacciones económicas de diversa índole, al igual que con cualquier otra moneda, y la segunda es la producción o "minería de bitcoins".

· **Realización de transacciones económicas:**

Siguiendo a González (2013), lo primero que necesitamos para realizar transacciones con *Bitcoin* es poseer una cartera o monedero, también conocidas como Bitcoin Wallets, que no deja de ser un archivo que necesitamos para guardar el valor de nuestras criptomonedas. Este archivo realmente lo que posee son nuestras claves criptográficas, claves privadas, únicas, irrepetibles y secretas, que nos hacen dueños de nuestros bitcoins y nos permite autorizar pagos.

Figura 5: Monedero electrónico Coinbase.



Fuente:

[monederos-fisicos-de-bitcoin-que-son-y-como-funcionan-a-la-hora-de-proteger-tus-inversiones](#)

Según González (2013) ``Una vez elegido un monedero digital donde guardarlos, existen diversa formas de obtener las criptomonedas a través de transacciones económicas``:

Sitios de compra-venta de Bitcoins: el más utilizado es MtGox. Pero hay muchos otros sitios que facilitan el intercambio de todo tipo de divisas por Bitcoin y admiten diversos sistemas para transferir los fondos. Algunos ejemplos son ``Bitinstant``y ``Bitcoin-Nordic``y que venden Bitcoins a través de cientos de miles de puntos de venta distribuidos en todo el mundo.

Sitios que aceptan oro y plata a cambio de Bitcoins: como, por ejemplo, ``coinabul``.

Aceptar bitcoin como pago por bienes o servicios: es posible fijar un precio en cualquier moneda y optar por ajustarlo automáticamente. Por medio de ``Bit-Pay``, los pagos en bitcoins además pueden ser automáticamente convertidos a la moneda que el usuario elija.

Encontrar a poseedores de carteras dispuestos a vender Bitcoins: se trata de mineros que disponen por lo general de grandes cantidades y que, son localizables en websites como ``tradebitcoin.com`` o foros especializados.

También hay empresas que pagan Bitcoins por determinadas acciones que realicen usuarios: la publicidad en webs o jugar a juegos en los que se obtenga como recompensas Bitcoins.

- **La segunda vía es la producción mediante la ``minería de bitcoins``:**

La segunda vía es la producción mediante la ``minería de bitcoins``, pero antes de presentarla es necesario definir el proceso de minería. La web ``bitcoin.org`` lo define como el proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados. Esta vía se beneficia del diseño de mineros operando a nivel mundial y sin ningún control absoluto sobre la red de un individuo u organismo.

Este proceso se denomina minería, como analogía a la minería del oro, en donde los *miners* obtienen nuevos bitcoins a través de servicios útiles que son necesarios para que la red de pagos funcione de manera segura. Siguiendo a Valkenburgh (2014), la minería de Bitcoin seguirá siendo necesaria hasta que se haya emitido el último bitcoin. ``Cuando se extrae oro, nada se logra más allá del descubrimiento de oro nuevo. Sin embargo, cuando se extraen bitcoins, se proporciona un servicio valioso a la red de Bitcoin: registro y validación de transacciones descentralizadas``.

Los mineros comprueban dos cosas cuando reciben una solicitud. Primero comprueban que realmente la firma digital ratifica que hayas sido anteriormente el destinatario de dichos inputs (es decir, que son tuyos). En segundo lugar, comprueban que ese monedero posea el dinero y no se hayan gastado esos inputs. Para realizar esta segunda comprobación, en la cadena de bloques, se comprueban todas las transacciones válidas ya efectuadas, para ver si esos inputs ya se utilizaron en una transacción o si todavía están disponibles. Las copias de la cadena de bloques se almacenan en el software de los dispositivos de todos los usuarios Bitcoin que se conectan a la red.

Continuando con Valkenburgh (2014), los mineros desempeñan el papel de los cajeros de banco: inspeccionan los cheques, asegurándose de que todo su contenido es correcto, comprobando la identidad del cliente y asegurando que este posee el suficiente efectivo para realizar la transacción.

El minero añadirá las transacciones válidas a su lista personal de todas las transacciones válidas en los últimos minutos. Cada pocos minutos, se seleccionará un minero para agregar su lista personal, un bloque, a la cadena de bloques oficial, manteniendo así el registro público

actualizado. Este minero seleccionado es recompensado con un determinado número de *Bitcoins*.

3.5 PERFILES DE USUARIOS

Siguiendo a Ennis(2016), encontramos cuatro perfiles diferenciados de usuarios Bitcoin, aunque en términos generales ``el usuario promedio es de 32 años de edad, de sexo masculino y libertario``. Desde la perspectiva de estos cuatro perfiles, los motivos de adhesión a Bitcoin encontrados por Ennis (2016) son:

- Para los especuladores, la volatilidad.
- Para los defensores de las libertades, la falta de regulación percibida.
- Para los delincuentes, el anonimato.
- Para los informáticos, las recompensas por la minería.

4. METODOLOGÍA

4.1 BITCOIN COMO MÉTODO DE PAGO

En esta sección se repasa la literatura sobre el papel de Bitcoin como medio de pago. En primer lugar, se presenta una panorámica histórica sobre los medios de pago virtuales, poniendo especial atención en el caso del bitcoin. En segundo lugar, se revisa la literatura académica centrada en el bitcoin como sistema de pago.

4.2 COMPARACIÓN PRINCIPALES MÉTODOS DE PAGO

A modo de introducción cabe señalar que en la actualidad se dispone de diferentes métodos de pago, según el medio en el que nos encontremos cuando realizamos compras; virtuales y físicos. Con Bitcoin podemos realizar ambas, siempre que sea aceptado por el vendedor. Cuando vamos a realizar pagos intentamos que sean lo menos complejos posibles, que las transacciones se realicen en el menor tiempo y los costes de estas sean preferiblemente nulos.

El estudio Ecommerce (2015) elaborado por lab España, revela que Paypal es la forma preferida de entre las electrónicas por el 64% de los españoles, debido a la privacidad con la que realizan las transacciones y la seguridad que esto reporta a los consumidores. Le siguen las tarjetas de crédito y débito con un 25% de cuota de utilización y ,por último, la compra contra reembolso con 7%. Lo que sugiere que apenas hay usuarios de criptomonedas monedas utilizandolas como medio de pago.

Mora (2016) repasa los principales métodos de pago. Así, menciona que, **Paypal** nació en 1998 y en 2002 fue adquirido por eBay, en la actualidad es uno de los sistemas de pago más empleados. Lo que hace PayPal es mediar entre el comprador y el vendedor, sin dar a conocer los datos del comprador. Entre sus ventajas destacan la rapidez, en la que sólo se necesitan los datos de acceso de Paypal y la flexibilidad, ya que se puede ingresar el dinero en Paypal a través de tarjeta, transferencia u otra cuenta de Paypal. Lo negativo son las comisiones para el vendedor (comisión variable entre el 1.9% y el 3.4%, más 0,35 \$ por transacción) y para el comprador, si en el proceso se produce cambio de divisas.

En lo que refiere al **pago con tarjetas**, son herramientas de pago plásticas, numeradas y magnetizadas, emitidas por entidades bancarias legítimas que autorizan a su portador a utilizarlas como medio de pago en negocios adheridos al sistema. La materialización del pago se realiza a través de la pasarela de pago (TPV virtual), que es la versión online de los datáfonos. El dinero se recibe por adelantado y es una forma de pago inmediata. Entre los inconvenientes de estas operaciones, encontramos que la entidad emisora de la tarjeta puede aceptar o rechazar la operación y, finalmente, la tienda online podría admitir o no la compra. Además, este método, posee comisiones para el vendedor.

Continuando con las criptomonedas, Mora (2016) indica que el bitcoin es un modelo de pagos online que está revolucionando internet, ya que, no se trata de un banco ni empresas intermediarias. Puede utilizarse para diversos tipos de transacciones, desde pagar productos en una tienda como enviar dinero al otro extremo del mundo. Sus ventajas, ya señaladas en la sección 2, son la descentralización y la conversión inmediata y sencilla de divisas, la protección de la identidad y la dificultad de rastreo de los fondos, la imposibilidad de su falsificación y sobretodo y por lo que es elegido por diversos usuarios es la incapacidad, de que los fondos sean intervenidos o congelados de manera arbitraria. Sus inconvenientes radican en su método de generación, ya que genera escasez de oferta de Bitcoins y la imposibilidad de que las transacciones sean reversibles. También la posibilidad de pérdida de los Bitcoins en el caso de perder u olvidar las claves privadas de acceso de tu *wallet*. Consciens (2018), sugiere la gran variedad de herramientas que facilitan la tarea de aceptar pagos con Bitcoin y criptomonedas, siendo en su mayoría totalmente gratuitas. Entre las más populares se encuentran Bitpay, Coinbase Commerce y coingate. Para finalizar con el método de pago virtual de los Bitcoins, seguimos a Wilson (2018), que señala que la tecnología *Blockchain*, donde se registra y valida de manera pública la actividad del Bitcoin, solo puede procesar una fracción de las transacciones

por segundo, evidenciando el uso masivo poco práctico de esta criptomoneda. Esta limitación de capacidad de procesamiento sería un inconveniente adicional de *Bitcoin*.

En definitiva, las principales diferencias radican en la intermediación, los costes de transacción y la rapidez de las operaciones.

En lo que se refiere al pago en tiendas o establecimientos utilizando Bitcoin. Coinsciens (2018), indica que ``los monederos móviles son uno de los métodos más fáciles para aceptar pagos con criptomonedas en tu tienda física, solo necesitas utilizar un *smartphone* o una tablet``. Estas carteras de criptomonedas (también conocidas como *wallets*) funcionan generalmente bajo unos mismos patrones, en primer lugar se ingresa el monto que el cliente debe pagar, generando esta *wallet* privada del dueño del negocio un código QR. El cliente escanea el código usando su *smartphone*, confirmando de esta manera la operación. Entre las ventajas de usar este tipo de monederos encontramos la facilidad de uso, en la que Coinsciens asegura que posee un uso muy similar e incluso más sencillo que la plataforma Paypal, ya que en menos de un minuto se puede estar enviando y recibiendo pagos. También destaca la seguridad de estos pagos en tienda con Bitcoin, dado que se utilizan medidas de seguridad adicionales como el doble factor de autenticación (2FA) o contraseñas de acceso. Otra ventaja es el escaso coste de mantenimiento, ya que la mayoría de wallets son gratuitas y las actualizaciones y mantenimientos constantes, manteniendo el soporte activo.

Las *wallets* con mayor uso se dividen entre iguales entre los sistemas operativos con mayor uso a nivel mundial. Por parte de iOS nos encontramos con Breadwallet, construida y diseñada sobre la base de seguridad de iOS para protegerse del malware, problemas de seguridad del navegador y robos físicos, con la que siempre tendrás acceso a tu dinero. Greenaddress, por su parte, utiliza nuevas direcciones para cada nueva transacción entrante, opciones para límites de gasto, doble factor de autenticación y multifirma para cada transacción realizada. En cuanto al sistema operativo Android destacan bitcoin Wallet, monedero fácil de usar , rápido y sin un servicio centralizado que valide las operaciones y transacciones y Mycelium, considerado uno de los monederos más rápidos de código abierto para Android. Su almacenamiento offline(*cold wallet*), añade un mayor nivel de seguridad a los bitcoins de usuarios fuera de línea.

4.3 INVESTIGACIÓN COMO MÉTODO DE PAGO EN WEB OF SCIENCE

En este trabajo de fin de grado se ha llevado a cabo una búsqueda en la base de datos WEB OF SCIENCE con el objetivo de conocer el estado de la cuestión, en relación a Bitcoin y, en especial, a su potencial como medio de pago. Al realizar la búsqueda en por el campo único de *Bitcoin* se obtuvo un total de 1754 salidas, de las cuales 230 se corresponden al área de Economía y Finanzas. Esto da una idea del creciente atractivo de *Bitcoin* en el mundo académico. Sin embargo, cuando se añade como segundo campo en esa búsqueda ``medium of

exchange'' (método de pago), el número de salidas de WOS se ve dramáticamente reducida a 13 resultados. Esto muestra un interés reciente, pero aún escaso acerca del análisis del bitcoin en cuanto a la función primigenia del dinero, es decir, servir como medio de pago.

Tal y como manifiestan Luther y Salter (2017), en Chipre en 2013, tras la necesidad de un rescate se anunció que se aceptaría imponer un impuesto único a los depósitos bancarios. Esto hizo que las cuentas tradicionales de depósito fueran menos seguras. El anuncio del rescate llevó a algunos a considerar o reconsiderar el uso de Bitcoin, sobre todo en aquellos países que tenían problemas con sus bancos, aunque finalmente no fue tan pronunciada la utilización de éstas. Baur, Hong y Lee (2018) analizan la cuestión de si Bitcoin es un medio de intercambio o un activo, cuál es su uso actual y qué uso prevalecerá en el futuro dadas sus características. Estos autores determinan el análisis de los datos de transacción de las cuentas de Bitcoin, demostrando que los Bitcoins se utilizan principalmente como una inversión especulativa y no como una moneda alternativa y un medio de intercambio. Por su parte, otros autores como Butek (2016), describen los límites en el uso de Bitcoin como medio de intercambio. La operación de la red bitcoin se lleva a cabo con altos consumo de energía eléctrica, que, con el tiempo, se reflejarán en el precio de las transacciones. Los bajos precios de transacción, que es uno de los incentivos para utilizar bitcoin, solo son posibles con la emisión continua de nuevos bitcoins a la circulación. La red ``peer-to-peer'' en la que se sustenta Blockchain es uno de los sistemas más exigentes en cuanto a demanda de energía, de entre todos los métodos existentes que aseguran las plataformas de cifrado. Continuando con Butek, otro de los impedimentos que aseguran el futuro de Bitcoin es ``El *halving*'' que reduce las recompensas de los mineros, este crea presión para disminuir la tasa de hash, que es un reflejo de la tasa de seguridad de la red. La presión para disminuir la tasa de hash está por ahora superada por la creciente eficiencia de los dispositivos de minería.

Siguiendo a Arsov(2016), los últimos años han sido testigos de los avances de los sistemas de dinero electrónico, como Bitcoin, Paypal y varias formas de pago mediante tarjetas. Además de identificar algunas de las características esenciales de los diferentes sistemas de pago, recalca el poder de bitcoin como mecanismo de pago. Esto es debido a que esta moneda posee unas características propias que la potencian como un sistema de pago totalmente inexistente en la historia de los hombres. En comparación con la mayoría de las monedas o los servicios de pago en línea, como Paypal, los Bitcoins son altamente líquidos y poseen bajos costes de transacción, pudiendo utilizarse para pequeños pagos. Este autor se centró en investigar cómo Bitcoin, la moneda de terminación digital complementaria, puede proporcionar una posición de respaldo sustentada en plataformas e-Gold, las cuales finalmente no proporcionan un medio de intercambio viable debido al coste de su compra, creación y/o intercambio. Continuando con otros investigadores encontramos a Cheang (2015), este nos muestra Bitcoin desde su introducción, y como esta moneda ha experimentado un aumento en el precio y su uso global, acompañado de enormes fluctuaciones de su precio, generando volatilidad y evidenciando en un

determinado momento su uso para la especulación. Este autor redonda en las afirmaciones de que Bitcoin se ha caracterizado por burbujas listas para reventar en cualquier momento, llevando a cabo una investigación econométrica de la existencia de burbujas en el mercado de bitcoin basada en una técnica desarrollada recientemente en la detección de burbujas. Detectando en el período 2011-2013 burbujas de corta duración y tres burbujas considerables en la última parte del período 2011-2013 que duraron de 66 a 106 días.

Por otra parte encontramos a Hong, Park y Yu(2018), estos analizan un régimen de doble moneda con moneda fiduciaria y dinero digital, en el marco del modelo económico monetario tradicional. Estos autores llevan a cabo un experimento de convivencia de una moneda fiduciaria y otra digital, concluyendo que se produce exclusión de una de ellas bajo supuestos de costos extremadamente altos asociados con el uso (medio de intercambio y almacenamiento de valor) de una moneda y costos extremadamente bajos asociados con el uso de la otra moneda.

De estas investigaciones llegamos a la conclusión conforme a las limitaciones que encontramos al utilizar Bitcoin. Principalmente su uso como medio de pago sólo se plantea cuando falla el sistema actual de dinero fiduciario, y llegando a este punto finalmente no obtiene un uso masificado por parte de los usuarios como medio de intercambio, evidenciando su utilización baja en la práctica.

Por otra parte, el objetivo por el que fue originado Bitcoin, que es el ser un sistema sustitutivo al dinero fiduciario como método de pago ha perdido poder frente a otra característica que fue desarrollando esta moneda, que no es otro que su alta volatilidad en el precio. Este alto valor especulativo, ha originado que sea utilizada por muchos inversores con otros fines, en detrimento de su utilización método de pago.

Otra limitación importante de esta criptomoneda es su minado, este método de recompensa genera altos costes energéticos. Aún no se ha evidenciado como una limitación ya que el beneficio obtenido es mayor a su coste de producción, aunque en un futuro desencadenará aspectos inciertos en la consolidación de esta moneda.

5. CONCLUSIONES

Bitcoin en sus inicios se planteó como un método de pago alternativo que pudiese hacer frente a la lentitud, centralización y falta de privacidad que presentan los métodos tradicionales. Sin embargo, la desconfianza creciente de la población global respecto a los sistemas monetarios actuales llevaron a que Bitcoin se utilizase más como una inversión y protección de capital. Con la inestabilidad de precios que presentó este nuevo tipo de moneda, la compraventa fue un desafío en muchos momentos. No obstante, con el paso del tiempo bitcoin ha creado una confianza en torno a su funcionamiento como moneda, otorgándole estabilidad, lo que muchos esperaban que tuviese para ser tratada como una moneda más fiable. Parte importante de la estabilización del precio del Bitcoin ha sido sin duda su cada vez mayor uso como **método de pago**, en vez de inversión acumulativa.

Desde su creación Bitcoin ha tenido tanto detractores como simpatizantes, en parte propiciado por el uso que le otorgaban sus usuarios (como por ejemplo el uso dado para pagar de manera anónima sustancias estupefacientes sin ser posible la identificación de los individuos por parte de las autoridades). Debido a este uso global creciente, determinados países se han visto en la tesitura de aceptarla como moneda legal, entre ellos Japón. Grandes empresas a nivel mundial también aceptan Bitcoin como método pago, entre las más importantes está Windows y instituciones como Europol estudian la implantación como método de pago en la unión europea. Siguiendo con este aspecto, en muchos países de la Unión Europea se espera un marco regulatorio sobre las criptomonedas. El gobierno Español ha confirmado que las criptomonedas están exentas del impuesto al valor añadido y bancos como BBVA y Bankinter invierten en empresas de Bitcoin.

Muchas instituciones financieras son reacias a aceptar Bitcoin como moneda legal, impulsado por la posible pérdida del sistema actual, hacia un nuevo modelo que no pueden controlar, aunque muchas han cogido la idea de este tipo de dinero y estén pensando en crear nuevas criptomonedas controladas bajo su supervisión. Desde la perspectiva económica y social, se ha creado un espacio totalmente nuevo, donde es difícil pronosticar qué efectos tendrá y si será totalmente aceptado. También citar diferentes obstáculos para que Bitcoin tenga un uso generalizado como moneda: la volatilidad, la aceptación política y la confianza. Un impedimento fundamental en su utilización como método de pago, es el hecho de que muy pocas instituciones lo reconocen y por otra parte nos encontramos con la cualidad primigenia del ser humano de no fiarse de lo novedoso y seguir sus costumbres y más aún cuando un elevado número de la población no sabe qué son exactamente términos como ``criptomonedas``, ``Bitcoin`` o ``Blockchain``.

A pesar de un futuro incierto, en parte debido a las fluctuaciones de su precio, lo que sí está claro es que cada vez más, Bitcoin es utilizado para pagar en materia de ámbito cotidiano, tanto a través de la web como físicamente en tiendas.

6. BIBLIOGRAFÍA

- Alonso, J. M.(2015). Un primer acercamiento al bitcoin.En Martín Fernández,J.(coord.)`Todo sobre Bitcoin: aspectos económicos, fiscales, contables y administrativos.`(23-24).Francis Lefebvre, Madrid.
- Antonopoulos,A.(2014).Mastering Bitcoin:Unlocking Digital Cryptocurrencies(pp.56-65).United States of America.Published by O'Reilly Media.
- BANCO CENTRAL EUROPEO.The ECB's definition of euro area monetary aggregates.[hist_content.en.html](#).Recuperado el día 25/2/2019.
- BANCO CENTRAL EUROPEO(2015). ¿Qué es el dinero?. [what_is_money.es.html](#). Recuperado el día 3/3/2018.
- Bankia.(2016). Historia del dinero: del trueque a las criptomonedas. Bankiaelblog.[historia-del-dinero-del-trueque-a-las-criptomonedas.html](#). Recuperado el día 30/4/2019.
- Bit2me.(2018). Precio histórico del Bitcoin.[precio-historico-bitcoin](#). Recuperado el día 21/4/2019.
- Cabezas, A.(2018).Masa monetaria y dinero¿qué son M0,M1,M2,M3 y M4?.IMF Bussines School.[masa-monetaria-dinero](#). Recuperado el día 21/03/2019.
- Castillo, A.(2018).Tipos de dinero:del fiduciario al electrónico.EAE Harvard School.[tipos-de-dinero-del-fiduciario-al-dinero-electronico](#). Recuperado el día 20/03/2019.
- Criptolog.Criptografía Bitcoin. ¿Qué es y cómo funciona?.[criptografia-bitcoin](#). Recuperado el día 6/5/2019.
- Criptotario.(2018).Criptomonedas respaldadas por oro.Criptotario.[criptomonedas-respaldadas-por-oro](#). Recuperado el día 21/6/2018.
- Consciens,A.(2018).¿Cómo aceptar pagos con Bitcoin y criptomonedas?.Tucryptomonedas.com. [aceptar-pagos-con-bitcoin-y-criptomonedas](#). Recuperado el día 01/07/2019.
- Delgado,V. Palacios,R.(2006).Introducción a la Criptografía:tipos de algoritmos.Researchgate.[28106424 Introduccion a la Criptografia tipos de algoritmos](#).Recuperado el día 30/04/2019.
- Díaz,G.(2018).Aprende las diferencias entre bitcoin y el dinero fiduciario.Criptonoticias.[aprende-diferencias-bitcoin-dinero-fiduciario](#). Recuperado el día 7/5/2019.
- Ennis.P(2016).The four types of Bitcoin users.Coindesk.com.[four-types-bitcoin-users](#). Recuperado el día 23/06/2019.
- Ernesto,B.(2019).¿Estamos cerca de otra crisis mundial?. Bitcoin está preparado. Bitcoin.es.[estamos-cerca-de-otra-crisis-mundial-bitcoin-esta-preparado](#).Recuperado el día 21/3/2019.

- González, J.M.(2013).Bitcoin. La moneda del futuro. Qué es, cómo funciona y por qué cambiará el mundo(pp.147-152). Madrid.Unión Editorial.
- Herrera, C.(2018).Qué es el Halving?.Tekcrispy.[halving-bitcoin](#). Recuperado el día 10/5/2019.
- IAB SPAIN.(2015).Estudio eCommerce 2015 elaborado por IAB Spain.IAB Spain.net.[Estudio-ecommerce-2015-IAB-abierta1.pdf](#). Recuperado el día 30/06/2019.
- Krugman, Paul R. y Wells, Robin.(2007). Macroeconomía: introducción a la Economía, Editorial Reverté.
- Leal, A.(2017). Europol estudia uso de Bitcoin como método de pago en la Unión Europea.Criptonoticias.[europol-estudia-uso-bitcoin-metodo-pago-union-europea](#). Recuperado el día 24/07.2019.
- Mankiw, Gregory.(2009). Principios de economía, Cengage Learning Editores.
- Mora, L.(2016).7 tipos de pagos online para online para eCommerce.[7-tipos-pagos-online-ecommerce](#). Recuperado el día 29/06/2019.
- Nieto, A.(2018).Cuál es la diferencia entre criptomonedas, moneda virtual y dinero digital. *Xatarka*.
- Ramirez Solano, E.(2007)Moneda, Banca y Mercados Financieros, Pearson Educación.
- Rosembuj, T.(2015).Bitcoin.El Fisco.[BITCOIN-1-a-156.pdf](#).Recuperado el día 20/04/2019.
- Satoshi Nakamoto.(2009).P2P. <https://www.diariobitcoin.com/index.php/glossary/dash>. Recuperado el día 7/5/2019.
- Valkenburgh, P.V.(2014).What is Bitcoin Mining, and Why is it necessary. Valkenburgh.[what-is-bitcoin-mining-and-why-is-it-necessary](#). Recuperado el día 5/5/2019.
- Vega, G.(2018).Cadena de bloques.Guía básica para entender qué es eso del ``Blockchain``.ElPaís.[1499945987_724507.html](#). Recuperado el día 24/6/2019.
- Wilson, S.(2014).Las cadenas de bloques tienen algo que ofrecer a la identidad?.Internet Society.org.[blockchain-identity](#).Recuperado el día 11/06/2019.

- **CONSULTADOS EN WOS:**
- Arsov, A.(2016). Bitcoin as an innovate payment currency in germany: Development of the e-Gold Standard.WOS.[full record.do](#). Recuperado el día 15/06/2019.
- Baur.D., Hong.H., Lee.A.(2018). Bitcoin: Medium of exchange or speculative assets.[full record.do](#).Recuperado el día 16/06/2019.
- Butek.M.(2016). Limits of use Bitcoin as a global means of exchange.[full record.do](#).Recuperado el día 27/06/2019.
- Cheang.A., Roca.E.,Su.J.(2015).Crypto-currency bubbles: an application of the Phillips-Shi-Yu(2013). methodology on Mt. Gox bitcoin prices.[full record.do](#). Recuperado el día 22/06/2019.
- Hong.K., Park.K., Yu.J.(2018). Crowding Out in a Dual Currency Regime? Digital Versus Fiat Currency.[full record.do](#).Recuperado el día 21/06/2019.
- Luther, W., Salter. A.(2017). Bitcoin and the bailout. [full record.do](#).Recuperado el día 22/06/2019.