FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TECNOLOGÍA DEL BLOCKCHAIN Y SU APLICACIÓN A LA EVOLUCIÓN Y PERSPECTIVAS DEL BITCOIN.

Trabajo Fin de Grado presentado por Elena Martínez Salas, tutorizado por Francisco Barbero Quesada.

Alumna: Vº. Bº. del Tutor:

Fdo.: Elena Martínez Salas Fdo.: Francisco Barbero Quesada

Sevilla, mayo de 2019

ÍNDICE

INTRODUCCIÓN

En este Trabajo de Fin de Grado analizaremos un tema de candente actualidad como es el de la criptomoneda, más concretamente el Bitcoin, al ser esta la primera, la de mayor repercusión mediática y la más conocida por el público en general.

Para poder analizar con propiedad este tema nos resulta necesario hacer una breve exposición de los pilares conceptuales y tecnológicos en los que se sustentan las distintas criptomonedas, incluyendo por tanto el Bitcoin, siendo el más importante de estos la tecnología conocida como blockchain.

Aunque la tecnología blockchain ya es de por sí un tema amplio y complejo, y que además engloba principalmente áreas del conocimiento que no son el objetivo a tratar en este Trabajo de Fin de Grado, intentaremos, por tanto, explicar lo fundamental para comprender el comportamiento del Bitcoin en términos económicos.

Desde hace varios años lleva siendo habitual encontrar noticias acerca del Bitcoin; aun así siguen existiendo muchos mitos al respecto y la falta de información y conocimiento sobre qué es realmente el Bitcoin y los usos para los que se creó son abundantes. Uno de los objetivos de este Trabajo de Fin de Grado será el de esclarecer si el Bitcoin ha cumplido los objetivos que marcó su creador.

Resulta conveniente señalar que el Bitcoin apareció en el año 2009 y que la coyuntura económica favorecía una desconfianza generalizada hacía las instituciones financieras y, por tanto, una mayor tendencia a buscar alternativas ajenas a un mercado centralizado y dominado por dichas instituciones. Esto resultó en el caldo de cultivo ideal para que surgiese una moneda descentralizada que, al menos en lo popular de su uso, tuviese éxito.

Sin embargo, la popularidad de uso no es lo que determina que un activo financiero pueda ser considerado una moneda. Teniendo en cuenta que con la creación del Bitcoin lo que se intenta es llegar a ser una alternativa practica y plausible al dinero fíat, plantearemos como objetivo principal de este Trabajo de Fin de Grado estudiar el Bitcoin desde distintos ángulos para poder discernir si ha acabado obteniendo la función con la que fue concebido.

CAPÍTULO 1: METODOLOGÍA Y ESTRUCTURA

La metodología utilizada para realizar este Trabajo de Fin de Grado será el empleo de datos publicados en la página web Blockchain.info, así como el uso de artículos académicos, trabajos y libros que abordan los temas relacionados con la blockchain y el bitcoin para poder desarrollar el marco teórico que sustenta el resto del trabajo. Además, usaremos los datos obtenidos de Blockchain.info para confeccionar tablas y gráficos mediante el uso del programa Excel. Para complementar y profundizar estos datos emplearemos también la información obtenida en distintas páginas web especializadas, las cuales están referenciadas en la bibliografía.

Para poder analizar de forma estructurada los objetivos de este Trabajo de Fin de Grado y alcanzar el objetivo que nos hemos marcado anteriormente, este Trabajo está dividido en tres capítulos, conclusiones y bibliografía.

Después de este primer capítulo, el segundo se centra en la tecnología blockchain que hace posible la descentralización que caracteriza a todas las criptomonedas. Para ello, este capítulo está subdividido en tres apartados: funcionamiento del Blockchain, tipos de Blockchain y elementos claves. Algunos de estos elementos claves serán vitales para entender el funcionamiento del Bitcoin como el minado o las redes peer-to-peer.

En el tercer capítulo analizaremos el Bitcoin en profundidad desde el punto de vista de la oferta y la demanda, así como la evolución del precio del Bitcoin ya que resultan de gran importancia para poder llevar a cabo el análisis del Bitcoin como moneda.

Por último, en el apartado de las conclusiones entraremos a valorar si realmente ha podido establecerse como una moneda alternativa al dinero fíat o si simplemente se ha convertido en un activo de uso especulativo.

CAPÍTULO 2: BLOCKCHAIN

Se trata de la tecnología o el sistema de codificación de la información que está por detrás de la moneda virtual y que sustenta toda su estructura[1]. Es una base de datos distribuida entre diferentes participantes, organizada en bloques de transacciones relacionados entre sí y que no puede ser alterada puesto que está protegida criptográficamente[2]. En resumen, es una base de datos inalterable y descentralizada. Un sistema ideado para que usuarios que desconfían unos de otros puedan mantener un consenso sobre la veracidad e integridad de la información que se encuentra grabada en él. El consenso es precisamente la clave de un sistema blockchain; este es un aspecto que podría revolucionar nuestra comprensión del funcionamiento del mundo, ya que posee la capacidad para transformar sectores estratégicos de la industria e, incluso, de nuestra sociedad.

Otra forma de ilustrar la idea de la blockchain es verla como un gran libro de contabilidad en el que se escriben todos los movimientos de una moneda virtual en concreto (por ejemplo, el Bitcoin) y todas esas entradas contables se agrupan por bloques antes de escribirse en él, y una vez escrito no se puede modificar, aunque cualquiera puede leerlo.

La gran versatilidad de la blockchain le permite hacer frente a un gran número de amenazas, ya que proporciona robustez, seguridad y transparencia a grandes sistemas de datos. Estas incluyen desde filtraciones de información a manipulación malintencionada del contenido. Además, gracias a la seguridad ante amenazas que proporciona este sistema hace innecesaria la figura de un tercero que garantice la validez de las transacciones que se lleven a cabo en ella, lo que se traduce en una reducción de costes considerable.

Desde un punto de vista técnico, gran parte de la tecnología blockchain está constituida sobre criptografía elemental como las funciones Hash, la criptografía de clave pública o la firma digital. A continuación, y durante este capítulo, profundizaré en estos conceptos para poder llegar a una correcta comprensión del funcionamiento de la tecnología blockchain.

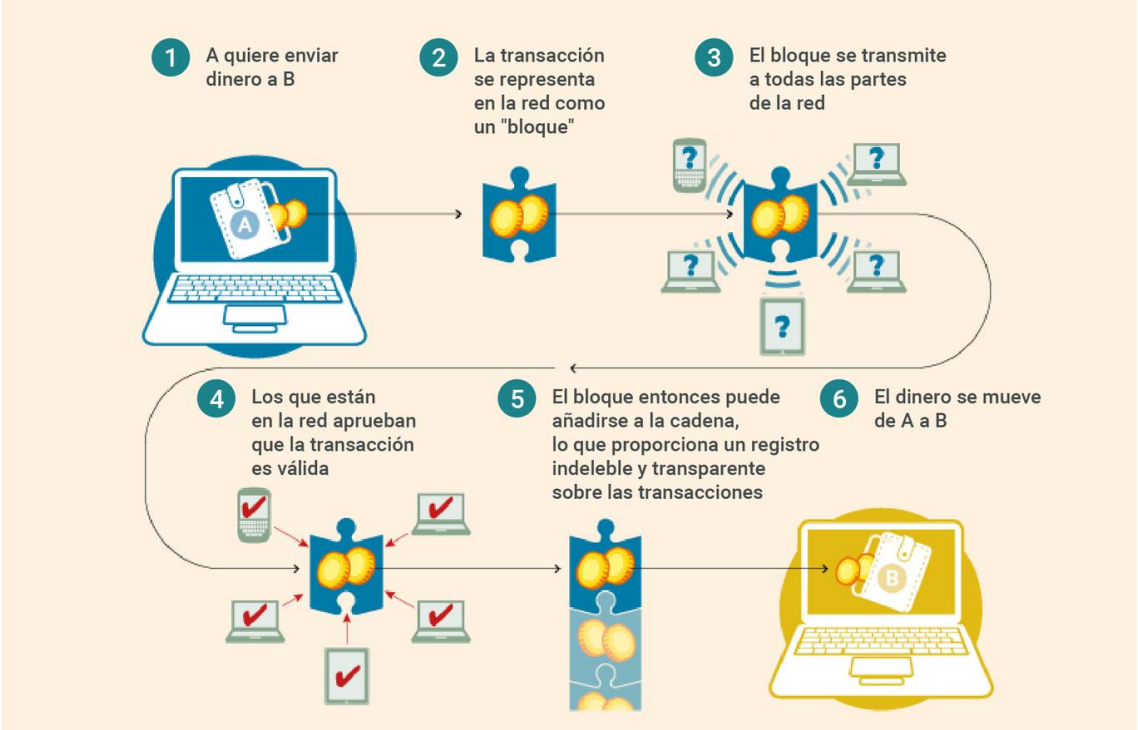
[1] https://www.imnovation-hub.com/es/transformacion-digital/que-es-blockchain-y-como-funciona-esta-tecnologia/
[2] Preukschat, 2017

2.1.- Funcionamiento de la blockchain

Esta tecnología soluciona el tradicional problema de la necesidad de un intermediario que verifique la autenticidad de las transacciones entre dos partes. Ahora bien, ¿cómo se soluciona este problema? Combinando la tecnología P2P y la criptografía.

De esta forma, si A quiere enviar dinero a B, esa transacción se representa en la red como un bloque y el bloque se transmite a todos los nodos de la red. Así, todos los integrantes tienen la información constantemente actualizada con todas las transacciones. Estos primero comprueban que la cartera de origen (A) tiene dinero para enviárselo a la cartera de destino (B). Si es así, todos anotan esa transacción, que pasa a completarse y a formar parte del bloque de transacciones. Sin embargo, todavía no están registrados en esa base de datos de forma definitiva. Con el tiempo, más transacciones van completándose y pasando a ese bloque. Cuando un bloque ya no admite más transacciones, hay que "validarlo" o "sellarlo", para ello, utilizamos una función de *hash* con unas características concretas para crear el sello.

Figura 2.1. Cómo funciona blockchain



Fuente: www.xataka.com

2.2. Tipos de blockchain

Hay que distinguir entre tres tipos de Blockchain públicas (o abiertas), privadas e híbridas.

En un principio, Blockchain fue diseñada como una tecnología de uso público donde cualquier persona sin ser usuario podía acceder y consultar las transacciones realizadas. Además, fue creada con un carácter abierto puesto que cualquiera puede convertirse en usuario y participar; sin una jerarquía entre los miembros de la red.

Posteriormente, surgieron las Blockchain privadas en las que no todos los datos tienen difusión pública y solo pueden participar quienes hayan sido invitados previamente. La principal diferencia entre una Blockchain pública y una privada está en la distribución de los nodos, puesto que en una blockchain pública la protección de esta se basa en gran medida en la cantidad de los nodos que la protegen y los incentivos que tienen para hacerlo, y en una Blockchain privada son los participantes quienes se comprometen a mantener la estabilidad del sistema.

En conclusión, la Blockchain pública (permissionless) es aquella cadena en la que cualquiera puede participar ya sea simplemente leyendo los datos o participando activamente en la validación de transacciones, mientras que la Blockchain privada (permissioned) es aquella en la que el proceso de consulta, validación y participación están limitados a unos nodos que previamente han sido invitados para poder participar.

Otra clasificación de la Blockchain que se puede hacer es según generaciones:

- **Primera generación:** el objetivo era la implementación de la tecnología de libro mayor distribuido (DLT) que consiste en un sistema de registro compartido donde poder ver todas las transacciones realizadas. Básicamente estaba pensado para realizar transacciones económicas y pagos en exclusiva.
- **Segunda generación:** se extiende la idea anterior con los contratos inteligentes que son programas informáticos que se ejecutan automáticamente siguiendo unas condiciones definidas de antemano. Estos contratos unidos a la tecnología blockchain son imposibles de manipular, por tanto, se supera el problema del riesgo moral.
- **Tercera generación:** aparece la idea de escalar el blockchain, lo que se busca solucionar es la lentitud con la que se procesaban algunas transacciones ya que todos los ordenadores de la red tenían que validarla. Para ello, se analizan cuantos ordenadores son realmente necesarios para procesar la transacción, manteniendo la seguridad que caracteriza al sistema blockchain.

2.3.- Elementos clave de la Blockchain

2.3.1.- Red Peer 2 Peer

Una red Peer 2 Peer es una red de ordenadores o nodos en la cual cada nodo se comporta de la misma manera, es decir, cada uno actúa tanto de cliente como de servidor.[3] Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Lo revolucionario de este tipo de redes es la robustez de este sistema ya que con que haya un solo nodo funcionando toda la red funcionará.

2.3.2.- Funciones hash

Como hemos dicho anteriormente cada bloque se "sella" con una función hash. Ahora bien, ¿Qué es una función hash? Hash es una palabra inglesa que significa "picar" o "moler", su significado en español está claramente relacionado con el concepto al que hace referencia, ya que, la criptografía consiste en "moler" contenidos hasta obtener una secuencia de caracteres fija.[4] Así pues, una función hash o "*digest*" es un algoritmo unidireccional que consigue, a partir de una entrada, una salida alfanumérica, de longitud fija que representa un resumen de toda la información que se le proporciona, algo así como la huella digital de un mensaje o documento.

Ejemplo 2.1. Resultado de aplicar una función hash a un mensaje

Mensaje	Resultado hash (hexadecimal)
«Perro»	5CDC4F3FEB31CEB78
«El perro de San Roque»	96C32852CB4C69E71
«El perro de San Roque»	20B003E7747353A6F

Fuente: Blockchain: la revolución industrial de internet.

[3] https://es.wikipedia.org/wiki/Peer-to-peer
[4] Preukschat, 2017

En la práctica, el hash se obtiene aplicando una función matemática a un conjunto de datos. Si la función y el texto no se modifican se obtiene el mismo hash, por lo que es especialmente útil para verificar la integridad de los datos.

De entre las características ya citadas, es importante recalcar el carácter unidireccional de las funciones *hash*. Una función unidireccional implica que una de las partes conoce el procedimiento de cálculo necesario para computar esa función, mientras que la otra lo desconoce por lo que es prácticamente imposible realizar ese cálculo a la inversa.

Una función *hash* tiene que tener una serie de propiedades para ser considerada segura:

- **Eficiencia de cálculo:** la función *hash* debe ser capaz de devolver rápidamente el hash de una entrada y a bajo coste.
- **Resistencia a preimagen:** que no se pueda prever el *hash* que se va a generar con un mensaje de entrada.
- **Resistencia a segunda preimagen y a colisión:** que sea muy difícil crear dos mensajes distintos que den como resultado el mismo *hash*. Teóricamente el hash es de menor tamaño que el mensaje de entrada por lo que podrían existir varios mensajes que dieran el mismo *hash*. Es lo que se conoce como colisión, si bien las buenas funciones hacen que algo así sea imposible.

2.3.3.- Criptografía

La criptografía consiste en transformar un mensaje legible en otro ilegible.[5] A este proceso se le llama cifrado, mientras que al proceso contrario es el descifrado. Esta ciencia resulta esencial para Blockchain, donde la información es compartida de forma encriptada por enormes redes de ordenadores sin ningún tipo de jerarquía.

Uno de los primeros métodos criptográficos conocidos es el sistema César[6], que consiste en desplazar cada letra del mensaje un cierto número de veces. Este método se conoce como encriptación simétrica puesto que se necesita conocer la clave tanto para encriptar como para desencriptar el mensaje y aquí radica la principal debilidad del sistema que tanto el emisor como el receptor tienen que conocer la clave para hacer posible la comunicación.

Para solucionar este problema se usa la encriptación asimétrica en los que el emisor y el receptor no necesitan compartir la clave. Este método se caracteriza por el uso de dos claves: una privada y una pública. La clave pública sirve para poder enviar mensajes cifrados, mientras que la clave privada sirve para

[5] Preukschat, 2017
[6] López Lérida y Mora Pérez, 2016

descifrarlo. Este es el sistema que se usa en la blockchain principalmente por la capacidad de garantizar la autoría del mensaje.

Para que este sistema funcione cada usuario tiene que poseer una clave pública y una privada. Por ejemplo, si Elena quiere enviar un mensaje a Paco tiene que conocer la clave pública de Paco que utilizará para encriptar el mensaje y ese mensaje solo se puede desencriptar con la clave privada de Paco por lo que quien no tenga acceso a la misma no podrá conocer el contenido del mensaje.

Las funciones de clave asimétrica son otro ejemplo de funciones unidireccionales, es decir, si conocemos la clave privada podremos averiguar la clave pública, pero si conocemos la clave pública no podremos averiguar la privada. La clave privada es un número aleatorio tan largo que hace que probabilísticamente resulte imposible generar otra igual y a partir de ella se calcula la clave pública mediante un algoritmo RSA (Rivest, Shamir y Adleman) o ECDSA (Elliptic Curve Digital Secure Algorithm).

Entrando más en detalle con el sistema criptográfico RSA, que es en la que se fundamenta el sistema ECDSA (utilizado por Blockchain), el funcionamiento de este algoritmo radica en el problema de la factorización de números enteros. Para ejemplificar este concepto imaginemos que nos dieran estas combinaciones de números 456,646,835,2345 y multiplicásemos sus cifras entre sí. Todas esas multiplicaciones aportarían el mismo resultado 120. Sin embargo, si nos dieran el número 120 (clave pública) no podríamos saber que combinación se ha utilizado (clave privada) para llegar a 120. Podríamos elevar la complejidad de este sistema utilizando grandes números primos.

No obstante, Blockchain hace uso de la criptografía de curva elíptica que no utiliza números primos sino coordenadas de una curva elíptica. Una de las ventajas de este sistema es que requieren números de menor tamaño que RSA para proporcionar el mismo nivel de seguridad, lo que hace que el algoritmo sea más rápido de procesar en la mayor parte de las operaciones.

2.3.4.- Firma digital

Otra peculiaridad de la encriptación asimétrica es que posibilita firmar un mensaje de forma que no se pueda dudar de su autoría, y esto se consigue mediante la firma digital que es uno de los elementos básicos sobre los que se constituye la blockchain, puesto que cada bloque contiene una serie de transacciones que constan de la firma digital del emisor y la clave pública del nuevo propietario.

Para ilustrar esta nueva aplicación de encriptación asimétrica volvamos a imaginar que Elena quiere enviarle un mensaje a Paco, pero esta vez no le importa que los demás conozcan su contenido, solo quiere que él esté seguro de que fue ella quien le envió el mensaje.

Para que Elena firme el mensaje tiene que seguir los siguientes pasos:

1. Crear un mensaje sin cifrar.
2. Aplicar una función *hash* obteniendo así un resumen del mensaje.
3. El *hash* es encriptado mediante su clave privada.
4. Finalmente, obtiene la firma digital del documento y se lo envía a Paco junto con el mensaje original que puede estar cifrado o no.

Para verificar la firma digital, cuando Paco recibe la firma y el mensaje:

1. Cuando se abre un documento en un programa que soporta las firmas digitales, este automáticamente usa la clave pública de Elena para desencriptar el documento *hash,* obteniendo así un resumen del mensaje tal y como fue computado por Elena.
2. Paralelamente se computa un resumen del mensaje que le ha llegado utilizando la función *hash* correspondiente.
3. Si ambos resúmenes coinciden la firma queda verificada, de forma que Paco puede estar seguro de que ese mensaje solo lo ha podido originar Elena y además ha llegado íntegramente.

2.3.5.- Proof-of-Work

Proof-of-Work, también conocido como prueba de trabajo, es un algoritmo matemático elaborado por Adam Back para el *HashCash* y que Nakamoto reutiliza para llegar a un acuerdo descentralizado que determina cuál de los bloques se agregará a la cadena.[7] Back creó un sistema destinado a dificultar la difusión de *spam* mediante la exigencia de un trabajo computacional previo al envío de un correo electrónico lo que haría prácticamente imposible el envío masivo de correo basura.

Las pruebas de trabajo de *Hashcash* se utilizan en Bitcoin para la generación de bloques. Los mineros[8] deben codificar las transacciones que aún no han sido verificadas con una función *hash,* pero la función que deben obtener tiene que cumplir con una serie de requisitos definidos por la red; por ejemplo, que la función resultante tenga que empezar por cuatro ceros. Por tanto, si queremos aumentar la dificultad computacional, una forma de hacerlo sería añadiendo más requisitos que tiene que cumplir esta función, como aumentar el número de ceros que debe tener.

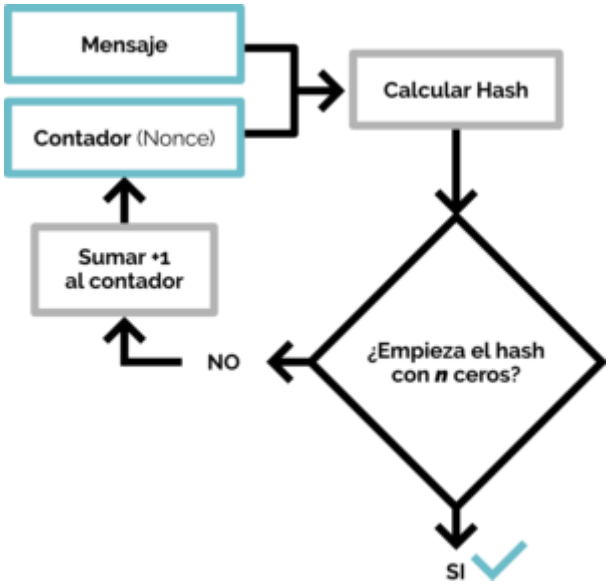
De esta forma, puesto que el resultado de la función *hash* no es predecible, la única forma de dar con uno concreto es mediante fuerza bruta, es decir, que los mineros tendrán que repetir muchas veces la operación hasta conseguir el resultado que cumpla las condiciones exigidas por la red. En cada nuevo bloque

[7] Cuartero, 2017
[8] Se conoce con este nombre a quienes realizan la minería.

de transacciones hay que añadir un contador llamado *nonce* que es un número aleatorio que cambia cada vez que se calcula un *hash;* de esta forma nos aseguramos de que el *hash* resultante es distinto en cada intento.

Una vez obtenido el *hash* que cumple los requisitos, la prueba de trabajo se da por satisfecha, el bloque se añade a la cadena y el contenido de este no podrá ser modificado sin rehacer el esfuerzo.

Figura 2.2. Proceso Hashcash para encontrar una prueba de trabajo



Fuente: Blockchain: la revolución industrial de internet

La Proof-of-Work también soluciona el problema del consenso dentro de un sistema descentralizado, y para ejemplificar este concepto y como se aplica a la blockchain vamos a explicar el problema de los generales bizantinos[9].

Se llama así porque plantea un supuesto en el que un grupo de generales de este antiguo imperio que están disperso y que deben ponerse de acuerdo para llevar a cabo un plan que solo tendrá éxito si todos atacan a la vez o se retiran. Supongamos que hay cuatro generales y que cada uno de ellos tiene un ordenador capaz de recibir y enviar mensajes, y de calcular hashes. Cualquier general puede proponer un plan y el plan que se envíe primero será el plan que seguir. Sin embargo, si dos generales envían el plan al mismo tiempo, algunos pueden recibir el plan A primero y otros pueden recibir el plan B, entonces para solucionar esta encrucijada se creó la cadena de trabajo que consiste en que los generales irán añadiendo sus votos a una cadena que representa un plan de forma que si hay dos planes habrá dos cadenas y tendrán que decidir cuál de las dos votar.

[9] Preukschat, 2017

Cuando un general decida emitir un plan pondrá a su ordenador a calcular un hash de una dificultad predeterminada como hemos indicado anteriormente cuando hablamos sobre el funcionamiento del *HashCash.* Así pues, el plan que más votos tenga, es decir, el que tenga un mayor esfuerzo computacional será el plan que se llevará a cabo. Si este esfuerzo proviene de una mayoría de nodos honestos la cadena honesta crecerá más rápido que otra originada por el ataque de unos nodos deshonestos, es decir, hay que suponer que los participantes tomarán sus decisiones pensando solo en maximizar su rentabilidad.

2.3.6.- Minado

La minería es el acto de verificar transacciones de criptomonedas dentro de una blockchain[10], es decir, cómo se generan los bloques dentro de la blockchain. Cada bloque contiene una serie de transacciones que los mineros tienen que validar y para lograrlo compiten entre sí con el poder computacional de sus ordenadores. El objetivo es crear un nuevo bloque lo más rápido posible y para ello deben adivinar el *nonce*.

Como se ha dicho en el apartado anterior, los mineros deben buscar una función hash que cumpla los requisitos exigidos por la red, es decir, deben ejecutar un algoritmo matemático complejo (PoW) con la información del conjunto de transacciones que configuran el bloque y con el *hash* del bloque anterior.

Una vez encontrada la solución, el bloque se añadirá a la cadena siempre que la mayoría de los mineros lleguen al consenso de que las transacciones registradas son válidas y que el minero ganador ha adivinado correctamente el *nonce*.

En cuanto al tiempo de generación de bloques, para aumentar la dificultad del minado hay que añadir más ceros al principio de la función hash. De esta forma, para mantener un tiempo de generación constante es necesario ir aumentando o disminuyendo la dificultad del *hash* requerido. Estos cambios serán realizados por los propios nodos y este proceso se llevará a cabo cada cierto tiempo o después de la creación de un número determinado de bloques según marque el protocolo establecido por la red.

[10] https://miethereum.com/mineria/

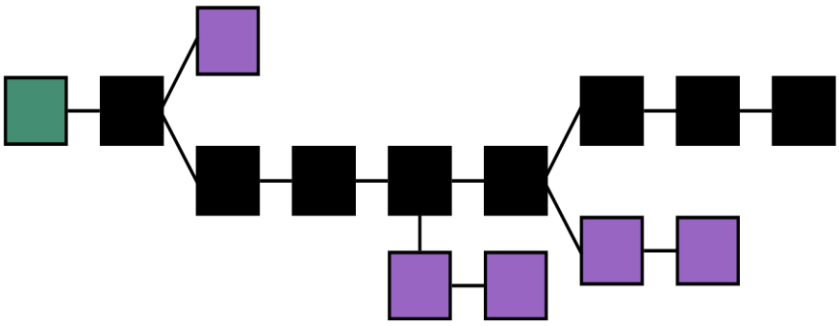
2.3.7.- Consenso (fork)

Como explicamos anteriormente PoW sirve para solucionar el problema del consenso (fork) en la blockchain, es decir, cuando dos o más mineros generan un nuevo bloque e intentan añadirlo a la misma cadena, simplemente se escoge la cadena más larga. Sin embargo, la cadena más larga no es la que tiene más bloques sino la que ha requerido un mayor esfuerzo computacional por parte de los mineros, puesto que la competencia entre ellos es lo que caracteriza la Proof -of- Work.

Si esto ocurriera, ¿a quién debemos recompensar?, ¿qué bloque elegir para el camino creado?, ¿qué pasaría si a unos usuarios les llega primero un bloque y al resto les llega el otro?

Para ejemplificar este concepto imaginemos que dos mineros, A y B, calculan el *nonce*, validan las transacciones y lo envían a la red casi simultáneamente. A la mitad de los mineros de la red les llega primero el bloque del A, y a los demás, el de B. En ese caso, parte de los mineros siguen trabajando con el bloque que les llega primero, por ejemplo, el de A, como si fuera el bueno y descartan el que les llega justamente a continuación. Esos mineros calculan más rápido el siguiente bloque de registro que los mineros a los que les llega el B. Así pues, los que estaban calculando el siguiente bloque a partir del B descartan esos cálculos y el bloque B entero, para seguir calculando a partir del bloque A y su subsiguiente[11].

Figura 2.3. Blockchain con cadena principal (bloques negros) y cadenas alternativas (morado)



Fuente: https://docs.blockcollider.org/docs/forks-and-reorgs

[11] Moreno, 2018

2.3.8.- Smarts Contracts

Un “Smart Contract” es un tipo de contrato que tiene la capacidad de cumplirse de forma automática una vez que las partes han acordado los términos[12]. Al igual que los contratos en papel constan del consentimiento voluntario de todas las partes, el objeto del contrato, y una causa. Ahora bien, ambos difieren en algunos aspectos como el modo de escritura o la forma de cumplirlo.

Los contratos inteligentes son programas informáticos, por lo que no están escritos en lenguaje natural sino en código virtual. Su cumplimiento no está sujeto a la interpretación de ninguna de las partes, sino que funciona como una sentencia: si el evento X sucede, la consecuencia Y se pondrá en marcha automáticamente.

El resultado es un acuerdo virtual blindado de manera que si todas las partes cumplen lo acordado no existirá posibilidad de fraude.

[12] https://www.criptonoticias.com/informacion/que-son-los-contratos-inteligentes/

CAPÍTULO 3: BITCOIN

En el capítulo anterior se ha explicado la tecnología blockchain, desde qué es hasta los elementos clave para su funcionamiento. Ahora bien, en lo referente a su aplicación económica, más concretamente a su uso como soporte de las monedas virtuales, no se puede negar su estrecha vinculación con el Bitcoin. Puesto que desde sus inicios la palabra blockchain ha sido asociada a Bitcoin, ya que fue la primera aplicación a la que dio soporte.

Por esta razón, para una mayor compresión del impacto que causó esta nueva forma de entender las transacciones económicas, es necesario comentar tanto el contexto en el que se originó como sus implicaciones económicas.

3.1.- Historia del Bitcoin

La aparición pública de Bitcoin se produjo el 1 de noviembre de 2008 con la publicación, en el dominio bitcoin.org, del *paper* titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”, escrito bajo el pseudónimo de Satoshi Nakamoto. Dicha publicación describe los fundamentos de la primera criptomoneda y la red que la sustenta.

Figura 3.1. Resumen de la publicación Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Fuente: https://bitcoin.org/bitcoin.pdf

Posteriormente, el 11 de febrero de 2009 en el portal P2P foundation, un usuario también con el nombre de Satoshi Nakamoto publicó un mensaje: "Bitcoin open source implementation of P2P currency". En el texto, se daba a conocer el portal oficial de Bitcoin, los elementos fundamentales que lo caracterizan, el artículo donde se describía el diseño e, incluso, el cliente inicial con el que comenzar a participar en la red.

Nakamoto combinó varias invenciones anteriores como b-money, que fue una propuesta fallida creada por Wei Dai, y Hashcash, inventado por Adam Back, con el objetivo principal de crear un sistema de efectivo electrónico totalmente descentralizado, el cual no dependa de ningún tercero que ejerza una autoridad central para su emisión, liquidación o validación de transacciones. Para solucionar el problema de las propuestas previas en este ámbito fue necesaria la gran innovación que supuso el uso de un sistema de computación distribuido para garantizar la seguridad de las transacciones, llamado algoritmo de prueba de trabajo o proof-of-work, el cual ya se explicó en el punto anterior. Con lo que se solucionó el problema del doble gasto, que permitía usar la misma moneda para dos transacciones distintas, siendo este el obstáculo en el que caían los intentos anteriores.

Satoshi Nakamoto se retiró de forma totalmente inesperada del proyecto Bitcoin en abril de 2011, legando la responsabilidad de desarrollar el código y la red a Gavin Andresen, quien a su vez también gobernó el desarrollo del proyecto hasta que decidió ceder la responsabilidad de este en abril de 2014 al holandés Wladimir van der Laan.

En cuanto a la identidad del creador, nunca se llegó a conocer hasta el punto de que ni si quiera si se sabe todavía si se trataba de una sola persona o de un grupo. Sin embargo, la perfección y complejidad del código hacen difícil que fuese un trabajo individual y esto ha dado alas a las teorías y especulaciones sobre que no podía tratarse de una sola persona. Lo cierto es que el código creado y la filosofía que hay tras él han revolucionado el mundo del software y de la economía, llegando incluso a ser nominado para el Premio Nobel de Economía 2016 por parte del profesor y doctor en finanzas Bhagwan Chowdhry, de la Universidad de California (UCLA). Aunque posteriormente la Academia de las Ciencias de Suecia rechazó esta nominación ya que el Premio Nobel no se puede otorgar a una persona anónima o que haya fallecido.

Actualmente, ni Satoshi Nakamoto, presuponiendo que sea una persona, ni nadie más posee el control del sistema Bitcoin, el cual actúa basándose en principios matemáticos donde la transparencia es el factor clave para su correcto funcionamiento. Además de que la idea fundamental de la creación de una moneda descentralizada como Bitcoin era librarse del lastre que supone tener que contar con la participación de un tercero que dote de confianza la transacción que se va a realizar, por lo que sería contraproducente que este sistema estuviese controlado por una persona o grupo de personas.

3.2.- Qué es el Bitcoin

Ahora que ya conocemos las bases teóricas en las que se sustenta la tecnología que usan las criptomonedas en la actualidad, el Blockchain, y además hemos hecho una breve introducción a la historia y el objetivo con el que se creó la primera y más importante criptomoneda, vamos a centrarnos ahora en el concepto mismo del Bitcoin.

El portal web oficial nos ayuda a abordar esta tarea, al darnos su propia definición:

"*Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet. Bitcoin puede ser el único sistema de contabilidad triple existente*[13]*.*"

Ahora bien, hay que aclarar qué es una moneda virtual y porque conceptualmente no es lo mismo que una moneda almacenada electrónicamente, como es el caso del dinero que tenemos depositado en el banco. Así pues, la moneda digital no es más que un código binario que hace referencia a una serie de transacciones producidas, y que queda registrada en una base de datos pública; es decir, que lo único que existe para respaldar el Bitcoin es un registro público de todas las transacciones producidas y las diferentes cuentas de los usuarios a las que se refieren esas transacciones. El sistema utiliza las transacciones procesadas en esta base de datos para determinar cuántos bitcoins posee cada usuario.

Esta ausencia de formato, es decir, la inexistencia de algo a lo que poder referirse y llamarlo Bitcoin, es la primera gran característica de la moneda digital. Por tanto, la base de esta nueva moneda digital se encuentra en la red, si esta sufre un ataque el bitcoin dejaría de existir.

Para el usuario final, el bitcoin es un medio de pago más como lo puede ser el euro. Los usuarios pueden usarlos para hacer prácticamente cualquier cosa que se pueda realizar con una moneda "tradicional", como comprar y vender bienes, enviar dinero a otros usuarios u organizaciones, e incluso extender créditos. Los bitcoins pueden comprarse, venderse e intercambiarse por otras monedas, por eso es la forma de dinero perfecta para internet.

Un único Bitcoin es denotado como 1 BTC y dado su naturaleza digital puede ser dividido hasta alcanzar 8 cifras decimales. Esto significa que la mínima cantidad de bitcoins que se puede poseer es 0,00000001 BTC, que como

[13] Pagliery, 2014

homenaje al creador se conoce como un Satoshi[14]. De esta forma las demás divisiones posibles también tienen su propia denominación:

Figura 3.2. Divisiones de un BTC

1 BTC	A bitcoin
0,01 BTC	A bitcent
0,001 BTC	An mbit
0,000001 BTC	A ubit
0,00000001 BTC	A satoshi

Fuente: Elaboración propia a partir de los datos obtenidos en el libro, Bitcoin: and the future of money.

3.3.- Oferta y demanda monetaria del Bitcoin

Una vez que ya hemos contextualizado su origen y en qué consiste realmente el bitcoin, es el momento de centrarnos en su implicación económica, y para ello se va a estudiar cómo se forma su oferta monetaria y los principales elementos que participan en la misma. De la misma forma, se analizará los determinantes de su demanda. La interacción de ambos análisis nos permitirá llegar a una conclusión sobre el comportamiento de su precio a lo largo del tiempo.

3.3.1.- Oferta monetaria de Bitcoins

La oferta de bitcoins, a diferencia de la moneda convencional, no es creada por un banco central o autoridad de ningún tipo. La creación de bitcoins es similar al proceso de extracción del oro. De ahí deriva el concepto de minería del que ya hablamos de forma genérica en el apartado correspondiente a la blockchain, y ahora procederemos a comentar su aplicación en el sistema bitcoin.

La minería es el acto de verificar transacciones de criptomonedas dentro de una cadena de bloques, y debido a la complejidad de este proceso se necesita un gran poder de procesamiento. De esta forma el incentivo para las personas que ponen a disposición sus equipos informáticos a la causa de la minería, es que al producir un bloque dentro de la cadena recibirá una cantidad estipulada de bitcoins en compensación por su trabajo.

La red genera un bloque cada diez minutos aproximadamente entre todos los usuarios que estén minando. Por tanto, alguien que tenga un equipo más potente tendrá más posibilidades de ganar. Esta dificultad de computación está regulada por el protocolo bitcoin publicado en 2009, siendo diseñado para que alcance un máximo de 21 millones de Bitcoins en el mercado en el año 2141, fecha a partir

de la cual no se generarán más aunque la fecha que es realmente importante es la de 2033, en la que según la progresión que lleva, el aporte de bitcoins por bloque descifrado se vería reducido hasta los 0,78 BTC con lo que sería cuando se estabilizaría la creación de moneda en el mercado.[15]

De esta forma es como el Bitcoin realiza la inyección de dinero en el sistema, pero un aspecto relevante a estudiar es el de la tendencia a que su oferta sea cada vez más rígida o fija. Esto puede generar que la economía bitcoin entre en deflación, es decir, que el poder adquisitivo aumente, probablemente hasta alcanzar dicha estabilidad. Lo más relevante es que la incapacidad de la oferta de dinero para adaptarse en función de la demanda probablemente provocaría una mayor volatilidad de los precios y la actividad real.

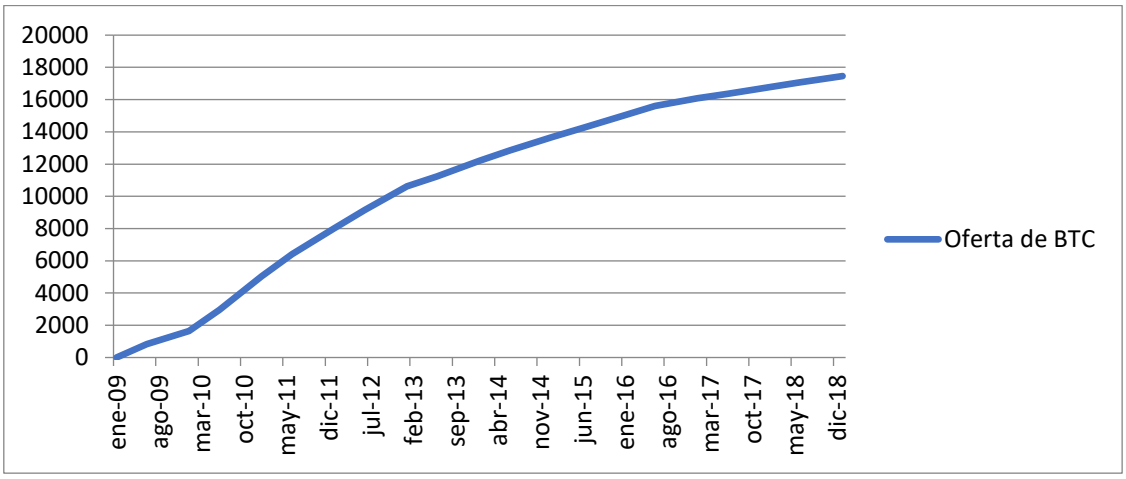
En el siguiente gráfico está representada la circulación en el mercado de los bitcoins, expresados en millones de unidades, en función del tiempo transcurrido desde que se crearon en 2009. Se puede observar que el ritmo de generación de nuevos bitcoins en el proceso de minado va haciéndose más lento según pasa el tiempo, sobre todo a partir de 2013 que es cuando se alcanzó la mitad de la oferta total. Debido a que en la actualidad se han minado 17.619.000 BTC, lo que es más de un 75% del valor final. Se estima que para 2033 se habrán minado un 99% de los bitcoins, pero como el ritmo de creación es más bajo hasta 2141 no se minará el último bitcoin.

Por otro lado, en la práctica, en algún momento entre 2033 y 2141 desde el punto de vista del minero que recibe una compensación en bitcoin por su fuerza de procesamiento la rentabilidad será muy baja[16]. Actualmente para obtener una mayor rentabilidad los usuarios se unen en los denominados “Pools de minería” para sumar así un mayor nivel de cómputo, y se repartirá el beneficio de forma proporcional al poder de procesamiento que aporte cada uno.

[15] González Otero, 2013

[16] https://www.xataka.com/criptomonedas/el-numero-de-bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces

Gráfica 3.1. Número total de bitcoin en circulación en millones de unidades. Años 2009-2018



Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

Tabla 3.1. Número total de bitcoins en circulación en millones de unidades. Años 2009- 2019

Fechas	BTC
03/01/2009	0,05
03/06/2009	823,4
03/01/2010	1644
03/06/2010	2960,6
03/01/2011	5044,45
03/06/2011	6419,9
03/01/2012	8023,2
03/06/2012	9143,05
03/01/2013	10625,175
03/06/2013	11238,125
03/01/2014	12211,525
03/06/2014	12851,45
03/01/2015	13682,825
03/06/2015	14231,6
03/01/2016	15035,4
03/06/2016	15613,45
03/01/2017	16079,338
03/06/2017	16367,963
03/01/2018	16778,588
03/06/2018	17071,05
03/01/2019	17459,488

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

3.3.2.- Demanda monetaria de Bitcoins

Una vez que hemos aclarado cómo se generan los bitcoins, la oferta, procederemos a hablar de la demanda de este. Para ello, la mejor forma es explicar el resultado de la interacción entre la oferta y la demanda, que es el cambio de valor sufrido por el bitcoin a lo largo del tiempo. Esta volatilidad en los precios de la que hablaremos en este apartado es una de las fuentes de conflicto en la consideración del bitcoin como moneda convencional o como activo para la especulación.

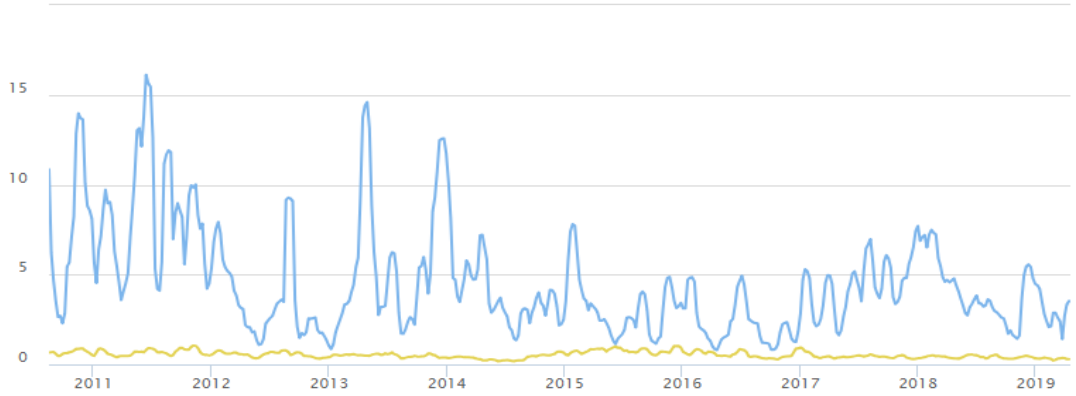
El precio de un bitcoin lo determina todo aquel que quiera participar en su proceso de compraventa, en esencia sus usuarios. Esto es lo que, en última instancia, determina siempre el precio del bitcoin, aunque para ello múltiples factores influyan[17]. Por tanto, cuando mucha gente compra bitcoins su precio tiende a subir (demanda), mientras que cuando mucha gente quiere vender sus bitcoins el precio tiende a bajar (oferta). Este tipo de tratos entre usuarios se lleva a cabo en plataformas especializadas conocidas como plataformas trading de bitcoins. En estas cualquiera puede publicar una propuesta de compra al precio que quiera y cuando otra oferta de venta coincida con la suya se hace la transacción. Por lo que no existe un precio oficial o único del bitcoin, aunque al ser instantáneos los envíos de bitcoin y, por tanto, la distancia no es un factor demasiado importante estos precios de compraventa tienden a equilibrarse.

Con respecto a su consideración como una moneda convencional es en su capacidad de depósito de valor donde no está tan claro su uso como dinero. Puesto que tiene que ser capaz de transportar del presente al futuro la capacidad de compra y el principal problema del bitcoin son sus fluctuaciones de valor con respecto al dólar. Al darse tanta variación en la cotización de la moneda, los usuarios no tienen ninguna certeza de que en un futuro sus ahorros valgan una cantidad de dólares determinada.

En el gráfico 3.2. podemos observar la evolución del índice de volatilidad del bitcoin con respecto al dólar desde el año 2011 hasta la actualidad comparada con el mismo índice entre el euro y el dólar. En él podemos apreciar las numerosas fluctuaciones que ha tenido el bitcoin a lo largo de los años. Mientras que el índice de volatilidad del dólar con respecto al euro, una moneda convencional o dinero fíat, se mantiene casi sin variaciones en el mismo período. Por tanto, y con estos datos, podemos afirmar que el bitcoin en la actualidad no cumple con la función de depósito de valor que debería poseer para poder ser considerado una moneda al uso como son el euro o el dólar americano.

[17] https://academy.bit2me.com/precio-bitcoin/

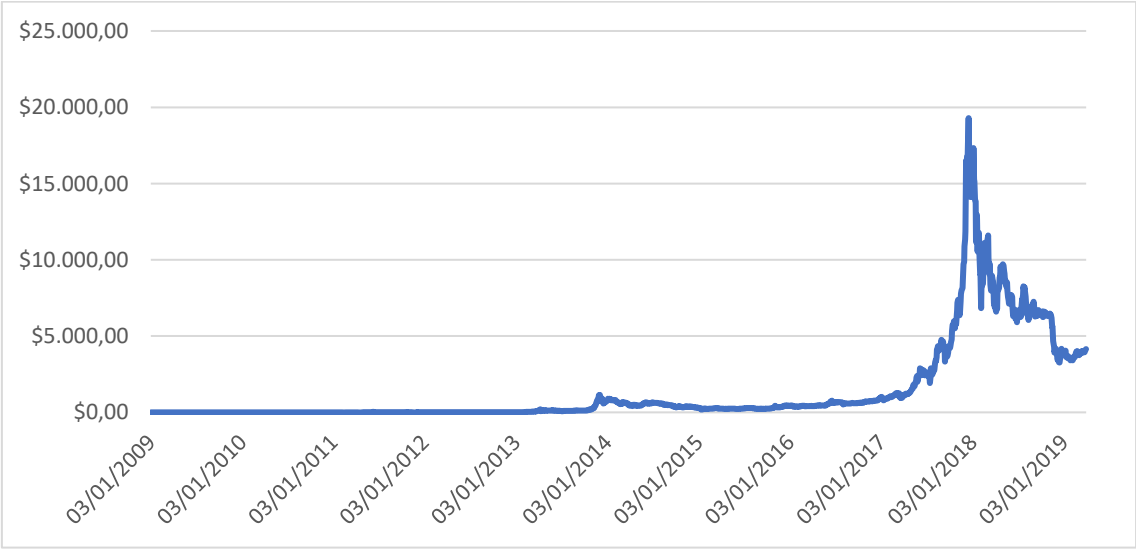
Gráfico 3.2. Comparativa de volatilidades — 30- Day BTC/USD Volatility — 30 Day USD/EUR Volatility. Año 2010-2019



Fuente: https://www.buybitcoinworldwide.com/es/indice-de-volatilidad/

En el gráfico 3.3. podemos observar cómo ha ido variando el valor del bitcoin desde su creación en 2009 hasta la actualidad. Hasta el año 2013 su precio no era relevante, pero sus fluctuaciones, aunque poco prominentes en términos absolutos, más aún teniendo en cuenta el valor máximo que ha llegado a tener el bitcoin cercano a 20000$ durante el mes de diciembre de 2017 como podemos observar en la gráfica 3.3, fueron muy grandes en términos relativos. Esto se puede observar tanto en el gráfico 3.2 anterior como en la tabla 3.3 donde se encuentra el valor promedio del bitcoin por año y por trimestre. Por ejemplo, en el primer trimestre de 2011 su valor promedio fue de 0,11$ y en el tercer trimestre del mismo año tuvo un valor promedio de 10,24$, casi 100 veces más.

Gráfico 3.3. Datos históricos de la cotización del bitcoin con respecto al USD. Año 2009-2019.



Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

En contraste con los primeros años es en 2017 y 2018 cuando el bitcoin experimenta sus mayores picos de valor, pero eso no significa que su volatilidad fuese necesariamente mayor. Al comparar ambas gráficas, en un primer momento puede parecer extraño que los mayores índices de volatilidad (gráfica 3.2.) se den entre los años 2011 y 2015, mientras que en la gráfica 3.3. en ese mismo periodo de tiempo no se observan apenas cambios. Esto se debe al que, al haber alcanzado cuotas de valor tan altas en los últimos años, los cambios de valor del bitcoin en sus primeros periodos anuales de existencia se han desvirtuado en la gráfica debido a la escala de esta. Por tanto, para poder hacer un análisis pormenorizado y exhaustivo tenemos que analizar la tabla 3.3. con la que se ha realizado la gráfica en cuestión.

Teniendo esto en cuenta, tiene mucho más sentido que el mayor índice de volatilidad se diese en los primeros años ya que observamos en la tabla 3.3. que en un mismo año el valor promedio puede llegar a ser hasta 100 veces más grande en dos trimestres distintos como sucede en el ejemplo anterior. Sin embargo, en los últimos años, aunque los valores absolutos resultan muy impactantes en comparación con los previos y la volatilidad sigue siendo bastante mayor que en comparación con una moneda convencional como el euro, esta ha disminuido sensiblemente. Un ejemplo de esto se puede observar si volvemos a considerar el trimestre de un año, en este caso del 2017 en el que valor promedio era $1.027,60 y lo comparamos con el tercer trimestre de ese mismo año, $3.513,04, siendo así el cambio de valor en ese periodo de tres veces su valor inicial. Mientras que en el mismo periodo de 2011 el cambio llegó a ser 100 veces del valor inicial del bitcoin en ese año.

Tabla 3.3. Evolución histórica de la cotización del bitcoin. Años 2011-2019.

Año/Trimestre	Promedio Cotización	Año/Trimestre	Promedio Cotización
2011	**$5,55**	**2015**	**$271,31**
1º Trimestre	$0,11	1º Trimestre	$250,22
2º Trimestre	$8,67	2º Trimestre	$235,64
3º Trimestre	$10,24	3º Trimestre	$254,74
4º Trimestre	$3,04	4º Trimestre	$343,39
2012	**$7,97**	**2016**	**$565,89**
1º Trimestre	$5,00	1º Trimestre	$409,74
2º Trimestre	$5,00	2º Trimestre	$510,47
3º Trimestre	$10,02	3º Trimestre	$614,28
4º Trimestre	$11,80	4º Trimestre	$727,85
2013	**$188,31**	**2017**	**$4.017,65**
1º Trimestre	$33,33	1º Trimestre	$1.027,60
2º Trimestre	$118,91	2º Trimestre	$1.901,24
3º Trimestre	$106,65	3º Trimestre	$3.513,04
4º Trimestre	$489,48	4º Trimestre	$9.563,72
2014	**$524,87**	**2018**	**$7.560,79**
1º Trimestre	$695,42	1º Trimestre	$10.502,16
2º Trimestre	$519,00	2º Trimestre	$7.777,11
3º Trimestre	$532,87	3º Trimestre	$6.795,57
4º Trimestre	$355,91	4º Trimestre	$5.236,98
		2019	**$3.781,48**
		1º Trimestre	$3.773,40
		2º Trimestre	$4.145,00

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

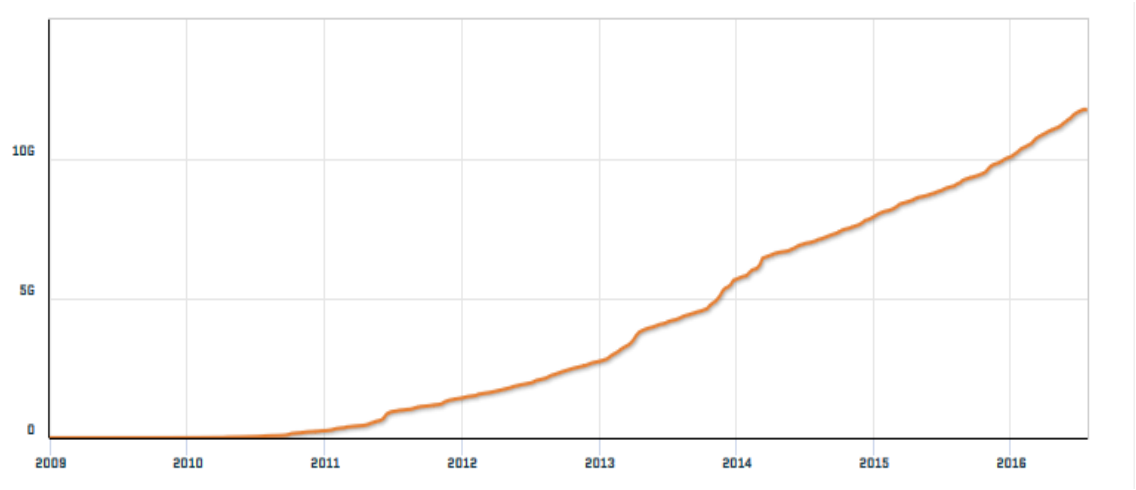
Esta gran variación de precios provoca un conflicto con su uso como moneda y su uso como inversión especulativa. Al no poder cumplir su función de depósito de valor, a lo que se une que durante la mayor parte del tiempo ha tenido grandes subidas, ha acabado siendo usado como un tipo de inversión especulativa. Sin embargo, el principal inconveniente de su uso especulativo es que el usuario trata de comprar lo más bajo posible y vender lo más alto lo que produce un efecto acaparamiento. Este acaparamiento viene definido como la cantidad de bitcoins que son retenidos como inversión frente al total de bitcoins en circulación.

Esta tendencia a atesorar bitcoins puede ser medida en términos de “coin-days destroyed”. Este término hace referencia en una transacción a la cantidad de tiempo que transcurre desde que se reciben unos bitcoins hasta que se gastan. Sin embargo, este concepto nace en 2011 en la comunidad bitcoin con el objetivo

originario de cuantificar el nivel de actividad económica de bitcoin, ya que cuando se analizan el volumen total de transacciones por día hay que tener en cuenta que hay transacciones que intentan inflar la actividad, y con esta fórmula no se cuantifica aquellas cantidades de bitcoins que se envían una y otra vez desde cuentas propias a lo largo de un día y en varias ocasiones[18].

La forma de calcular la destrucción de "coin-days" se obtiene multiplicando la cantidad gastada por el número de días transcurridos desde que esos bitcoins fueron utilizados por última vez. Por ejemplo, si 2 bitcoins no se han gastado en 10 días (2BTC x 10 días) en la gráfica de días de bitcoins destruidos contaría como que ese día se han movido 20 bitcoins. De esta forma podemos ver cuanta actividad real está habiendo en la economía bitcoin, ya que un número bajo de días destruidos significa que más bitcoins están siendo atesorados y, por otro lado, un número alto significa que muchas monedas están en uso.

Gráfico 3.4. Bitcoin days destroyed acumulados. Años 2009-2016.



Fuente: https://www.quandl.com

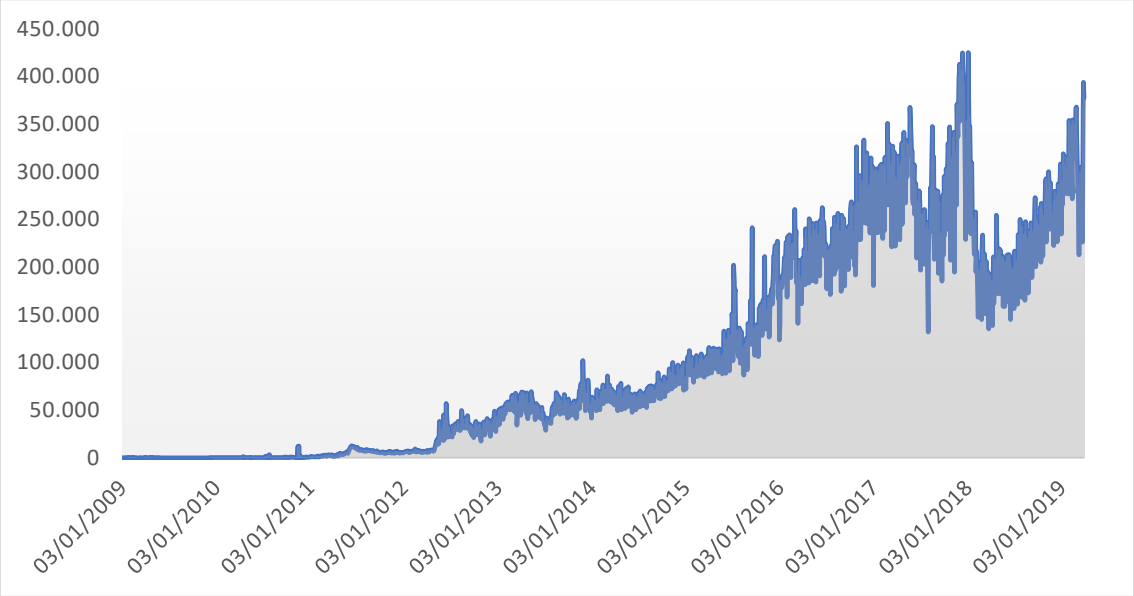
En la gráfica 3.4. podemos observar que existe una tendencia creciente del número de coin-days destruidos; esto quiere decir que su uso ha aumentado en estos últimos años. Este aumento puede ser explicado por diversos factores como el incremento de su popularidad y de su cotización o la concepción que tienen los usuarios de los bitcoins como un activo de alto riesgo, pero rentabilidad también elevada.

Esta tendencia creciente en el uso del bitcoin también se puede apreciar en el número de transacciones por día (gráfico 3.5.) que han aumentado considerablemente. Sin embargo, en 2018 cuando el bitcoin alcanzó su cuota máxima de valor (gráfico 3.3.) el número de transacciones diarias cayó drásticamente, puesto que en 2017 el promedio anual de transacciones por día llegó a estar en 52087846 en 2018 estaba en 40685433. Esta disminución en su utilización justo en el momento en el que su valor estaba más alto apoya la

[18] https://www.oroyfinanzas.com/2014/12/que-es-bitcoin-days-destroyed-dias-bitcoins-destruidos/

hipótesis de que los usuarios no utilizan los bitcoins como medio de cambio, puesto que, en vez de utilizarlos como medio de pago para adquirir bienes y servicios, decidieron atesorarlos para su uso especulativo.

Gráfico 3.5. Número de transacciones diarias en bitcoins. Años 2009-2019.



Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

Tabla 3.5. Evolución histórica del número de transacciones con bitcoin. Años 2009- 2019

Año	Nº Transacciones	Año	Nº Transacciones
2009	**16395**	**2014**	**12677842**
1º Trimestre	4758	1º Trimestre	2879772
2º Trimestre	4545	2º Trimestre	2888176
3º Trimestre	2821	3º Trimestre	3096974
4º Trimestre	4271	4º Trimestre	3812920
2010	**93581**	**2015**	**22819112**
1º Trimestre	8112	1º Trimestre	4318837
2º Trimestre	10614	2º Trimestre	4889192
3º Trimestre	25841	3º Trimestre	6047406
4º Trimestre	49014	4º Trimestre	7563677
2011	**951980**	**2016**	**41475007**
1º Trimestre	78315	1º Trimestre	9188564
2º Trimestre	270643	2º Trimestre	9991449
3º Trimestre	346724	3º Trimestre	10149838
4º Trimestre	256298	4º Trimestre	12145156
2012	**4213325**	**2017**	**52087846**
1º Trimestre	301237	1º Trimestre	12680910
2º Trimestre	919671	2º Trimestre	13422221
3º Trimestre	1486127	3º Trimestre	11239510
4º Trimestre	1506290	4º Trimestre	14745205
2013	**9779597**	**2018**	**40685433**
1º Trimestre	2359562	1º Trimestre	10039910
2º Trimestre	2400017	2º Trimestre	8729639
3º Trimestre	2257466	3º Trimestre	9994063
4º Trimestre	2762552	4º Trimestre	11921821
		2019	**13914536**
		1º Trimestre	13914536

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

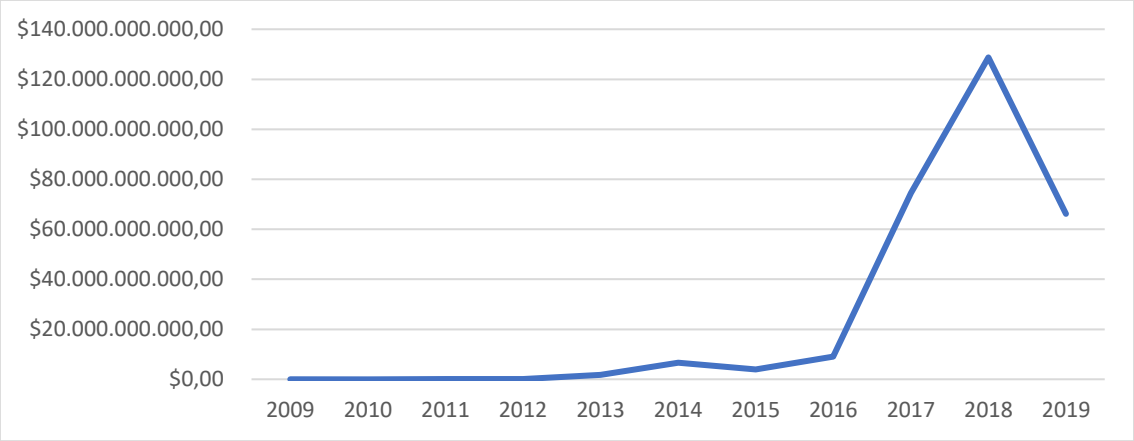
Para concluir este análisis, la forma más conveniente de enlazar la oferta y la demanda monetaria de bitcoins es la capitalización de mercado, la cual es el resultado de multiplicar el número de bitcoins en circulación (oferta) por su cotización actual (demanda). Este índice refleja el capital total de un proyecto criptográfico, es decir, expresa el dinero supuestamente invertido en este proyecto[19].

Como se puede observar en la gráfica 3.6., la capitalización del bitcoin ha tenido una evolución creciente prácticamente sin variación desde su creación hasta principio de 2018. Esto se debía principalmente a dos factores de los cuales ya hemos hablado siendo el más obvio de ellos el aumento del número de bitcoin en circulación siguiendo el protocolo previamente descrito en el punto 3.3.1. El segundo factor es por tanto la cotización de cada bitcoin, este segundo factor es el que explica las bajadas que ha sufrido la capitalización del bitcoin puesto que de los dos factores es el único que puede tanto incrementar como disminuir.

El ejemplo más visible de la influencia de este segundo factor se encuentra en la gran bajada de la capitalización desde el pico del primer trimestre de 2018. Actualmente esta capitalización se está equilibrando, y ya no se están observando subidas tan vertiginosas como las que se dieron en 2017 durante la fiebre del bitcoin y ni bajadas tan estrepitosas como las ya comentadas a principios del 2018.

En resumen, podríamos decir que esta gráfica nos aporta una visión conjunta sobre los datos observables tanto en la gráfica 3.1. como en la 3.3.

Gráfico 3.6. Datos históricos de la capitalización de mercado del bitcoin en USD. Año 2009-2019.



Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

[19]https://www.criptonoticias.com/opinion/que-nos-dice-capitalizacion-mercado-criptomoneda/

Tabla 3.6. Datos históricos de la capitalización del bitcoin en USD.

Años 2009-2019

Años/Trimestre	Promedio de Capitalización	Años/Trimestre	Promedio de Capitalización
2009	**$0,00**	**2014**	**$6.651.053.776,48**
1º Trimestre	$0,00	1º Trimestre	$8.476.650.198,79
2º Trimestre	$0,00	2º Trimestre	$6.754.235.186,59
3º Trimestre	$0,00	3º Trimestre	$7.106.398.259,67
4º Trimestre	$0,00	4º Trimestre	$4.826.956.587,89
2010	**$284.985,91**	**2015**	**$3.995.575.903,64**
1º Trimestre	$0,00	1º Trimestre	$3.480.619.835,24
2º Trimestre	$0,00	2º Trimestre	$3.384.725.826,47
3º Trimestre	$130.686,91	3º Trimestre	$3.769.021.902,50
4º Trimestre	$996.866,02	4º Trimestre	$5.223.512.470,91
2011	**$31.855.587,03**	**2016**	**$9.109.689.852,85**
1º Trimestre	$4.004.892,29	1º Trimestre	$6.285.798.458,28
2º Trimestre	$41.153.301,13	2º Trimestre	$8.086.408.897,59
3º Trimestre	$72.459.719,70	3º Trimestre	$9.787.352.126,55
4º Trimestre	$27.499.810,54	4º Trimestre	$11.819.083.268,00
2012	**$85.163.728,59**	**2017**	**$74.517.717.983,10**
1º Trimestre	$45.370.768,18	1º Trimestre	$16.480.398.999,33
2º Trimestre	$49.681.715,56	2º Trimestre	$32.643.350.394,44
3º Trimestre	$100.773.886,47	3º Trimestre	$58.042.250.277,54
4º Trimestre	$130.015.976,39	4º Trimestre	$162.418.087.101,32
2013	**$1.718.309.642,05**	**2018**	**$128.732.016.765,88**
1º Trimestre	$362.945.209,25	1º Trimestre	$177.710.362.628,85
2º Trimestre	$1.320.328.792,57	2º Trimestre	$132.587.645.209,47
3º Trimestre	$1.181.664.314,77	3º Trimestre	$114.737.503.583,78
4º Trimestre	$5.210.668.954,95	4º Trimestre	$91.888.303.515,02
		2019	**$66.192.522.907,44**
		1º Trimestre	$66.192.522.907,44
		Total general	$27.130.371.789,70

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

3.4. Evolución del valor de los bitcoins

Una vez estudiado el bitcoin desde la perspectiva de la oferta y de la demanda, y cómo la determinación de su precio se basa en el acuerdo al que llegan los propios usuarios, es conveniente centrarnos en la evolución del valor de los bitcoins, puesto que como ya se mencionó anteriormente es uno de los rasgos distintivos de esta criptomoneda.

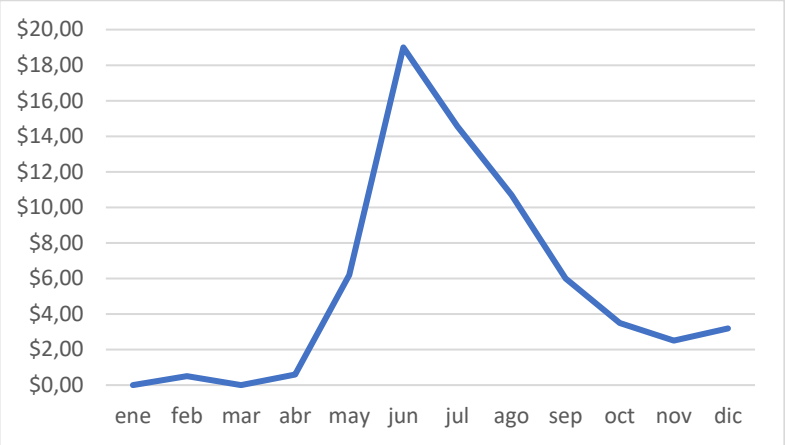
Lo que más llama la atención del gráfico 3.3. en el que se muestran los datos históricos de la cotización del bitcoin es que en los años 2017 y 2018 se alcanzan unos valores muy elevados, por lo que da a entender que en los primeros años esas fluctuaciones de valor no fueron significativas. Por esta razón, procederemos a analizar la cotización de cada año en particular con el objetivo de mostrar las verdaderas fluctuaciones que experimentó el bitcoin a lo largo de sus primeros años.

En el año 2009, momento de su creación, el bitcoin no tenía ningún tipo de valor puesto que los primeros usuarios simplemente se los intercambiaban en foros a modo de prueba, es decir, no intentaron adquirir en ningún momento un bien a cambio de un determinado número de bitcoins. Por lo que durante ese año su cotización se mantuvo en 0 dólares. No fue hasta el 22 de mayo de 2010 cuando se lleva a cabo la primera compra de un producto utilizando bitcoins. Un usuario con el pseudónimo de “Lazlo” compró una pizza por 10000 BTC (una pizza de 25 dólares USA).

El 11 de julio de 2010 la influyente página Slashdot.org sobre proyectos de código abierto publicó una breve nota sobre bitcoin, provocando la subida del precio desde menos de un centavo de dólar hasta los 7 centavos en unos pocos días[20]. Según pasaron los años se afianzó la confianza de los usuarios, unido a la desconfianza en el sistema monetario actual provocada por la crisis financiera, lo cual hizo factible la creación del primer sitio de trading de Bitcoin, Mt Gox, con sede en Tokio el 17 de julio de 2010.

[20] https://www.oroyfinanzas.com/2013/11/precio-bitcoin-cotizacion-2010-2011/

Gráfico 3.7.y Tabla 3.7. Cotización del bitcoin con respecto al USD. Año 2011



	Promedio cotización
Enero	$0,00
Febrero	$0,50
Marzo	$0,00
Abril	$0,60
Mayo	$6,20
Junio	$19,00
Julio	$14,55
Agosto	$10,70
Septiembre	$6,00
Octubre	$3,50
Noviembre	$2,50
Diciembre	$3,18
Anual	$5,61

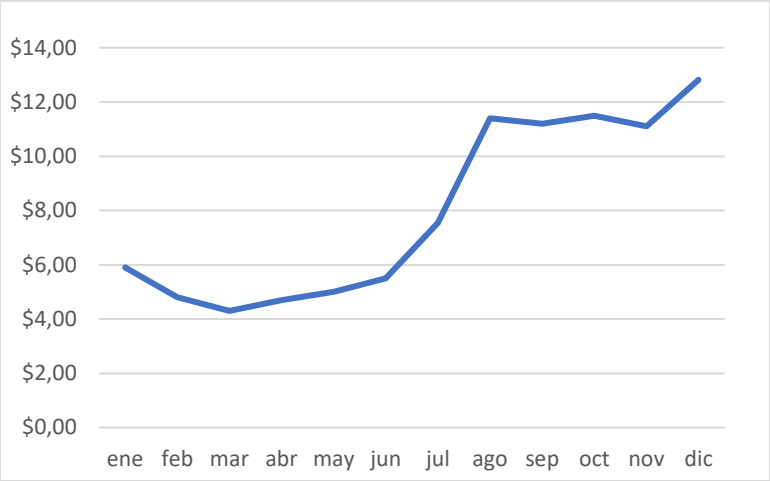
Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

En el año 2011 continua la tendencia creciente que experimentó en la segunda mitad del 2010. El 9 de febrero de 2011 el precio del bitcoin supera por primera vez el precio de un dólar y como podemos observar en el gráfico 3.7. se mantiene constante hasta comenzar a subir lentamente en el mes de mayo y alcanzar un pico de 31 dólares por bitcoin, pero cuatro días después el valor cae hasta los 10 dólares. En este punto tenemos un claro ejemplo de la alta volatilidad que caracteriza al bitcoin, ya que después de este alza comenzó un descenso que le llevó a alcanzar su punto más bajo en noviembre cuando se cotizó en 2 dólares[21].

En junio de 2011, la base de datos de Mt Gox sufre un ataque y se logra obtener el listado de 60000 usuarios con sus contraseñas. De la misma manera alguien accede a una cuenta de administrador de este mismo sitio de trading emitiendo órdenes de venta de bitcoins inexistentes, y forzando la caída de la cotización desde 17.51$/BTC hasta los 0.01$/BTC[22]. Este hecho queda reflejado en la gráfica 3.7. en la que se puede apreciar claramente el brusco descenso de la cotización que experimentó el bitcoin.

[21] https://www.criptonoticias.com/colecciones/altibajos-precio-bitcoin-historia/
[22] González Otero, 2013

Gráfico 3.8. y Tablas 3.8. Cotización del bitcoin con respecto al USD. Año 2012



	Promedio Cotización
Enero	$5,90
Febrero	$4,80
Marzo	$4,30
Abril	$4,70
Mayo	$5,00
Junio	$5,50
Julio	$7,55
Agosto	$11,40
Septiembre	$11,20
Octubre	$11,50
Noviembre	$11,10
Diciembre	$12,82
Anual	$8,02

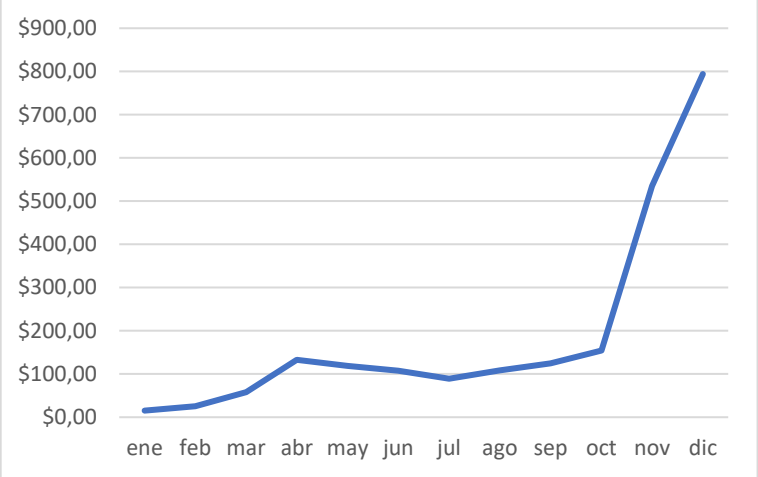
Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

En el año 2012 se aprecia una ligera recuperación del valor del bitcoin, aunque con un crecimiento más moderado en la primera mitad del año ya que como podemos observar en el gráfico 3.8. entre enero y julio el valor del bitcoin osciló entre los 4$/BTC y los 8$/BTC. En la tabla 3.8. se puede apreciar como el promedio del mes de julio de 2012 se mantuvo en 7.55$/BTC mientras que en ese mismo mes, el año anterior el promedio era el doble.

Tanto WordPrees.com anuncia su decisión de empezar a recibir pagos en bitcoins como LewRockwell, que también comienza a admitir donaciones en Bitcoins[23]. Estos hechos hacen que los usuarios vuelvan a depositar su confianza en la moneda y esto se ve reflejado en el segundo semestre de este año que consigue mantenerse con un promedio de 11$/BTC para cerrar el año con un valor de 13.51$/BTC.

[23] Mencheba Molongua, 2016

Gráfico 3.9. y Tabla 3.9. Cotización del bitcoin con respecto al USD. Año 2013



	Promedio Cotización
Enero	$15,30
Febrero	$25,22
Marzo	$57,91
Abril	$132,50
Mayo	$118,80
Junio	$107,40
Julio	$89,40
Agosto	$108,73
Septiembre	$124,80
Octubre	$154,30
Noviembre	$535,20
Diciembre	$794,10
Anual	$188,25

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

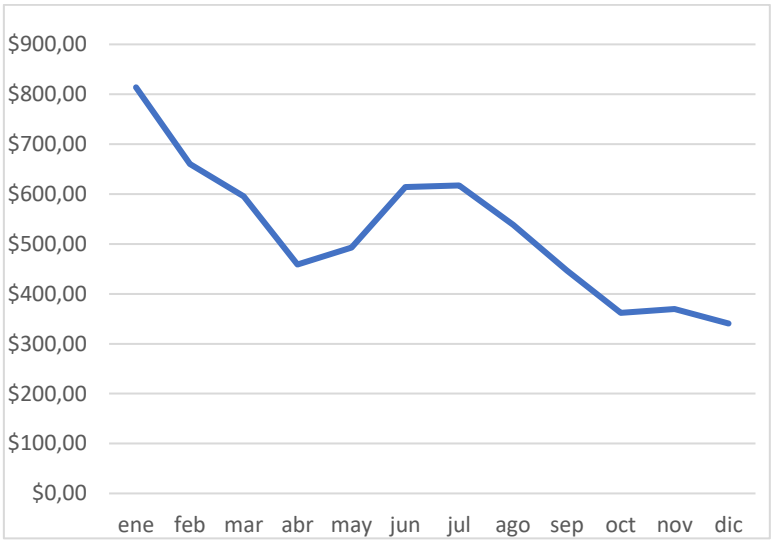
En el año siguiente se registra un marcado crecimiento en el valor del bitcoin. En el mes de marzo de 2013 el precio de bitcoin duplicó el precio máximo de 2012 de 15,25 dólares y en una semana subió un 50% más. Si comparamos las tablas 3.8. y 3.9 podemos observar como el promedio del mes de marzo de 2013 es 53.61 puntos porcentuales mayor que en 2012.

En el mes siguiente el precio del bitcoin se dispara llegando a alcanzar el 9 de abril los 230 $/BTC supuestamente esta subida se explicaría con el anuncio del corralito bancario en Chipre. Posteriormente, Mt Gox pone en entredicho la seguridad de la moneda, al recibir ataques DDoS. El motor de trading de Mt Gox se llegó a parar en varias ocasiones como consecuencia de los ataques, lo que al principio disparó los precios y posteriormente aceleró la caída. El objetivo de los ataques DDoS era hacer bajar los precios de Bitcoin en los sitios de intercambio respectivos para comprar en las caídas y después beneficiarse de las subidas cuando el problema estuviera resuelto, favoreciendo movimientos especulativos[24].

Otro mes notable en el 2013 es octubre. Aparece el primer cajero de bitcoins en Canadá, el FBI cierra Silk Road y detiene a su creador. A partir de noviembre continua la tendencia alcista cerrando el año en 757.49$/BTC y con un promedio del mes de 794.10$/BTC (Tabla 3.9.).

[24] https://www.oroyfinanzas.com/2013/11/precio-del-bitcoin-en-2013-el-ano-del-bitcoin-con-precios-maximos-historicos/

Gráfico 3.10. y Tabla 3.10. Cotización del bitcoin con respecto al USD. Año 2014



	Promedio Cotización
Enero	$813,91
Febrero	$660,11
Marzo	$595,50
Abril	$458,70
Mayo	$492,64
Junio	$614,20
Julio	$617,00
Agosto	$538,30
Septiembre	$446,60
Octubre	$362,09
Noviembre	$369,70
Diciembre	$340,60
Anual	$525,43

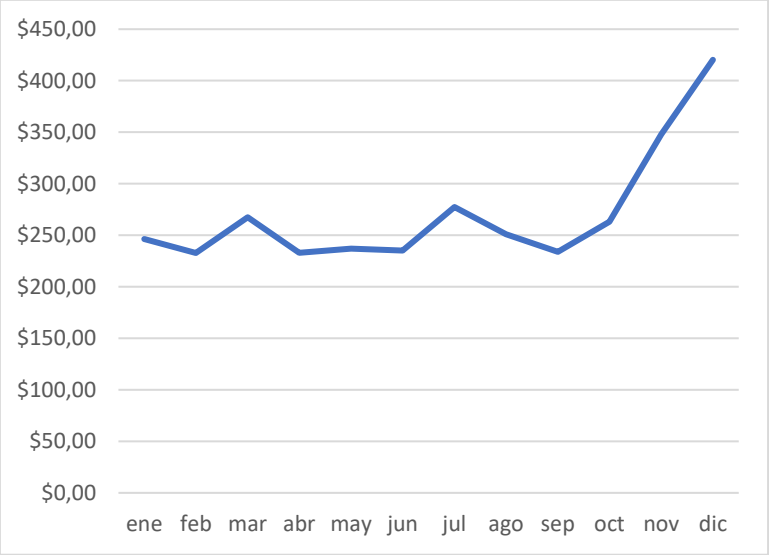
Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

La cotización del bitcoin comienza el año 2014 con la tendencia alcista del año anterior, pero como podemos apreciar claramente en el gráfico 3.10. aunque empezó con valores oscilaban entre los 700 y los 800$/BTC a lo largo del año fue descendiendo gradualmente.

De acuerdo con Anton Badev y Matthew Chen (2015), los acontecimientos importantes que marcan la evolución de la moneda en el 2014 empezarían en febrero del mismo año con el anuncio de la quiebra de Mt Gox, dando a conocer pérdidas de 850.000 bitcoins valorados en aproximadamente 500 millones de dólares. En este mismo mes, Bistamp (la considerada mayor bolsa de intercambio de bitcoins), tras sufrir un ataque de negación de servicios DDoS, paralizó los retiros varios días lo cual provocó una importante pérdida de confianza en la criptomoneda. La autoridad tributaria de Estados Unidos, el IRS, publica unas guías sobre las monedas virtuales en marzo. Así mismo en junio los reguladores de Nueva York hacen propuestas sobre nuevas normas que regulen los negocios de divisas virtuales[25]. Estas propuestas hacen que el Bitcoin pierda parte del atractivo principal que tenía, ser una moneda que no dependiese de ninguna autoridad centralizadora, gubernamental o no. El conjunto de esta pérdida de atractivo de la criptomoneda y, principalmente, de los ataques que sufrió, explican la tendencia a la baja que siguió manteniendo durante la segunda mitad del año.

[25] Mencheba Molongua, 2016

Gráfico 3.11. y Tabla 3.11. Cotización del bitcoin con respecto al USD. Año 2015



	Promedio Cotización
Enero	$246,20
Febrero	$232,80
Marzo	$267,60
Abril	$233,00
Mayo	$237,10
Junio	$235,30
Julio	$277,27
Agosto	$251,10
Septiembre	$233,90
Octubre	$263,00
Noviembre	$347,80
Diciembre	$420,27
Anual	$271,73

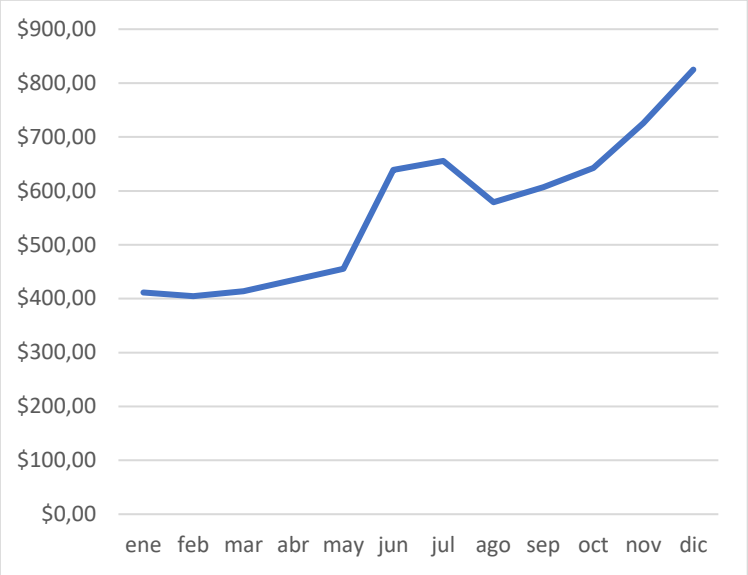
Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

Pese a la bajada que llevaba experimentando el Bitcoin a final del año 2014 comenzó el 2015 estabilizando su cotización durante la mayor parte del año en alrededor de 250 $/BTC como se puede observar en la tabla 3.11. El 21 de octubre de 2015 el Tribunal de Justicia de la Unión Europea dictó sentencia a raíz de una disputa producida en Suecia en junio de ese mismo año, ya que la agencia tributaria de ese país deseaba gravar las operaciones realizadas con bitcoin con un impuesto. El tribunal dictaminó que las operaciones tanto con bitcoin como con otras criptomonedas estarían exentas de impuestos[26].

Gracias a este hecho las criptomonedas recibían el mismo trato que otras monedas de curso legal en circulación, lo que aumentó su popularidad y supuso por tanto un gran impulso en su cotización, que mantendría esta tendencia alcista, con alguna breve bajada puntual en el siguiente año, desde finales de octubre de 2015 hasta alcanzar máximos históricos en diciembre de 2017.

[26] https://www.xataka.com/empresas-y-economia/europa-dicta-sentencia-bitcoin-y-otras-monedas-virtuales-quedan-libres-de-impuestos

Gráfico 3.12. y Tabla 3.12. Cotización del bitcoin con respecto al USD. Año 2016



	Promedio Cotización
Enero	$411,40
Febrero	$404,60
Marzo	$413,80
Abril	$434,50
Mayo	$455,40
Junio	$638,70
Julio	$655,82
Agosto	$578,70
Septiembre	$606,60
Octubre	$642,50
Noviembre	$725,40
Diciembre	$825,00
Anual	$568,89

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

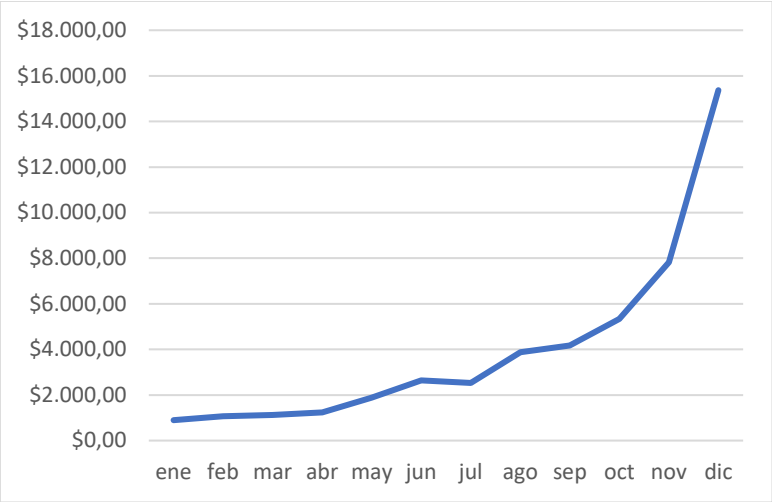
Con respecto al 2016 podemos apreciar tanto en la gráfica 3.12. como en su tabla de datos correspondientes como entre enero y mayo el valor del bitcoin se mantuvo constante. Sin embargo, en junio de este año varios acontecimientos han propiciado que se fortalezca la posición del bitcoin y como resultado su valor incrementó considerablemente.

Uno de los hechos que ha favorecido este tipo de moneda es la incertidumbre que golpea a las potencias económicas, puesto que ante la posibilidad de que Donald Trump asumiese el mandato, los inversionistas previeron la caída del dólar. Ante un posible periodo de debilidad de la divisa americana, las monedas virtuales se erigen como opción segura de inversión.

Otro motivo por el que el bitcoin ha ganado valor es la desmonetización de la India. En el país asiático, el gobierno decidió retirar los billetes de 500 y 1.000 rupias del mercado. La medida fue tomada como estrategia para combatir el dinero negro. Sin embargo, casi el 86 por ciento de las reservas de efectivo de ese país se encontraban conformadas por billetes de las denominaciones prohibidas, lo que ha derivado en un caos transitorio. Como resultado, el bitcoin se ha establecido como opción de inversión para la India, viéndose reflejado este hecho en un aumento de su valor[27].

[27] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/precio-del-bitcoin-en-2016-45452

Gráfico 3.13. y Tabla 3.13. Cotización del bitcoin con respecto al USD. Año 2017



	Promedio Cotización
Enero	$894,90
Febrero	$1.064,22
Marzo	$1.125,91
Abril	$1.238,10
Mayo	$1.880,80
Junio	$2.645,30
Julio	$2.525,70
Agosto	$3.882,27
Septiembre	$4.164,80
Octubre	$5.333,50
Noviembre	$7.820,90
Diciembre	$15.371,00
Anual	$3.995,19

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

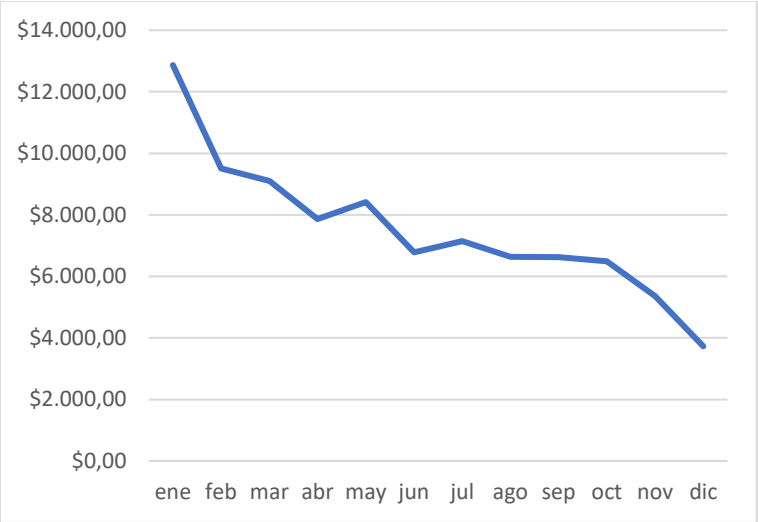
Durante el año 2017 tuvo lugar una serie de acontecimientos que provocaron una gran inestabilidad en su precio. Sin embargo, pese a su volatilidad y sus cambios radicales de valor consiguió mantener una tendencia alcista a lo largo del año.

En el gráfico 3.13. se observa que ese aumento en el valor del bitcoin es más acusado a partir del mes de agosto. Esto puede ser el resultado del nacimiento de Bitcoin Cash una bifurcación surgida a partir de su protocolo original. En un principio este hecho provocó una caída del valor del bitcoin pero el 12 de agosto pasa la barrera de los 4000$/BTC y el 14 de agosto toca máximo llegando a los 4400$/BTC[28].

A partir de julio de 2017 Corea del Sur, uno de los países donde más extendido está su uso, planteó la creación de un marco legal para su uso y el de otras criptomonedas. Esto provocó un gran aumento de su demanda y una subida constante de precios y que llegase a máximos históricos el 17 de diciembre con un precio de 21000 $/BTC[29].

[28] https://academy.bit2me.com/precio-historico-bitcoin/
[29] https://criptodinero.es/bitcoin/evolucion-del-precio-del-bitcoin-en-2017-2018/

Gráfico 3.14. y Tabla 3.14. Cotización del bitcoin con respecto al USD. Año 2018



	Promedio Cotización
Enero	$12.867,00
Febrero	$9.508,78
Marzo	$9.102,50
Abril	$7.864,60
Mayo	$8.418,36
Junio	$6.785,60
Julio	$7.148,40
Agosto	$6.635,70
Septiembre	$6.623,00
Octubre	$6.486,45
Noviembre	$5.352,40
Diciembre	$3.726,30
Anual	$7.569,30

Fuente: Elaboración propia a partir de los datos obtenidos de Blockchain.info

Aunque las perspectivas del bitcoin parecían bastante halagüeñas en el año 2017 distintos rumores y noticias de que el gobierno de Corea del Sur planeaba prohibir las operaciones con criptomonedas, provocaron una fuerte bajada que hizo que un solo día la capitalización del bitcoin bajase un 40%. Siendo el mayor mercado mundial de bitcoin la posible prohibición en Corea del Sur afectó notablemente al mercado.

Además, otros gobiernos como los de Alemania o de Francia también se plantean regular el bitcoin, lo que provoca que el año de 2018 sea de recesión para el mercado de bitcoin acabando el año en torno a los 4000$/BTC, a nivel de septiembre del año anterior.

CONCLUSIONES

A través de la realización este Trabajo de Fin de Grado hemos podido analizar la mecánica de la tecnología del blockchain y enlazarla con el funcionamiento del bitcoin así como con su evolución a lo largo del tiempo. Una de las primeras herramientas con la que hemos medido el éxito del bitcoin ha sido la evolución del número de transacciones diarias, con ello hemos podido comprobar que ha tenido una gran penetración en el mercado, especialmente en el asiático. No solo es la criptomoneda con mayor número de transacciones diarias sino que además sigue manteniéndose como la criptomoneda con mayor capitalización incluso después de las constantes bajadas que sufrió durante todo el año 2018.

Uno de los mayores hitos que ha logrado el bitcoin está en el vertiginoso crecimiento que ha tenido en tan solo diez años. Incluso aunque parecía abocado al desastre a principios del 2018 cuando comenzó un descenso en su cotización desde el pico de 20000 $/BTC, en los últimos meses ha comenzado a estabilizarse e, incluso, aunque acabase desapareciendo no hay que negarle el logro de haber sido la primera criptomoneda en llegar al público general, consiguiendo llegar a un nivel de popularidad tal que algunos gobiernos hayan tenido que tomar medidas legislativas para regularizar su uso.

Todos estos logros han allanado el camino para que una importante cantidad de criptomonedas hayan salido con éxito al mercado. Sin embargo, como señalamos en la introducción, la popularidad de su uso no determina que pueda ser considerada una moneda; no obstante y como hemos analizado a lo largo del Trabajo hemos visto que podría ser una alternativa al dinero fíat. Este análisis previo era necesario para señalar que como mínimo ha logrado ser el primer obstáculo en el camino para conseguir una criptomoneda que funcione como alternativa al dinero convencional.

Más allá de este éxito inicial cuando estudiamos los objetivos con los que fue creada y en lo que se ha convertido, hemos podido observar una serie de divergencias que cuestionan su naturaleza como alternativa descentralizada a una moneda convencional. Aunque ha logrado mantener su carácter descentralizado a todos los niveles, emisión, liquidación y validación de transacciones, resulta más difícil afirmar que haya conseguido que su uso sea similar al del dinero fíat.

En este Trabajo de Fin de Grado hemos estudiado dos de las características fundamentales del dinero, como son el ser depósito de valor y el ser también un medio de pago o cambio; siendo el objetivo del bitcoin convertirse en un método de pago digital debería cumplir estas dos características.

Para analizar si cumple la función de depósito de valor hemos comparado su índice de volatilidad con respecto al del dólar USA. En esta comparativa ha sido evidente que la alta volatilidad del bitcoin, debido a sus grandes fluctuaciones de cotización, hace imposible que pueda cumplir la función de depósito de valor. Estas fluctuaciones generan una gran inseguridad al usuario y, además, hacen que sea imposible predecir el valor que tendrán unos hipotéticos ahorros en bitcoin.

En cuanto a su función como medio de pago, hemos visto que se llevan a cabo una gran cantidad de transacciones diarias, pero debido a estas fluctuaciones que hemos comentado no podemos saber si gran parte de ellas son únicamente con afán especulativo o si realmente se usan para adquirir bienes y servicios. El hecho de que el número de transacciones tuviese una bajada coincidente en el tiempo con la última gran bajada en la cotización, nos hace pensar que efectivamente gran parte de su uso era con fines especulativos, usándose el bitcoin más como activo financiero que como moneda.

Con todos estos datos y después de realizar este análisis podemos afirmar que aunque evidentemente el bitcoin ha conseguido grandes éxitos no ha logrado cumplir todavía el objetivo principal con el que fue creado.

Sirva este Trabajo Fin de Grado como una aportación al análisis de la tendencia creciente del uso de estas monedas virtuales en un mundo eminentemente globalizado, y también como punto de partida para la realización de otros trabajos en el futuro desarrollo de mi posterior actividad académica.

BIBLIOGRAFIA

Libros y artículos

- Cuartero, A. I. (2017). *Blockchain y su Aplicabilidad a una Industria bajo Regulación.*
- Franco, P. (2015). *Understanding bitcoin: Economics.* United Kingdom: Wiley Finance Series.
- González Otero, J. M. (2013). *Bitcoin. La moneda del futuro. Qué es, cómo funciona y por qué cambiará el mundo.* Madrid: Unión Editorial.
- Lasala, I. G. (2018). *Blockchain.La revolución de la industria.*
- López Lérida, J., y Mora Pérez, J. J. (2016). *La economía de Blockchain.* Creative Commons.
- Mencheba Molongua, J. (2016). *Bitcoin,¿la moneda del futuro?* Coruña: Facultade de Economia e Empresa da Universidade da Coruña.
- Moreno, G. M. (2018). *Blockchain: pasado, presente y futuro.* Barcelona.
- Pagliery, J. (2014). *Bitcoin: and the future of money.* Chicago: Thriumph Books.
- Preukschat, A. (2017). *Blockchain: la revolución industrial de internet.* Barcelona: Gestión 2000.
- Rodríguez, M. Á. (2015). *El mercado de los bitcoins.* Sevilla: Facultad de Turismo y Finanzas.

Webs

- *A medium corporation* . (7 de Diciembre de 2017). Obtenido de https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666
- *Academy by bit2me*. (s.f.). Obtenido de https://academy.bit2me.com/precio-historico-bitcoin/
- *Academy by Bit2me*. (s.f.). Obtenido de https://academy.bit2me.com/que-es-minar-bitcoins/
- *Academy.bit2me*. (s.f.). Obtenido de https://academy.bit2me.com/precio-bitcoin/
- Bastardo, J. (Diciembra de 2018). *Criptonoticias*. Obtenido de https://www.criptonoticias.com/opinion/que-nos-dice-capitalizacion-mercado-criptomoneda/

- *Bitcoin.org*. (s.f.). Recuperado el 25 de Marzo de 2019, de https://bitcoin.org/es/faq
- *Block Collider*. (s.f.). Obtenido de https://docs.blockcollider.org/docs/forks-and-reorgs
- *Criptonoticias*. (s.f.). Obtenido de https://www.criptonoticias.com/informacion/que-son-los-contratos-inteligentes/
- *Criptotario*. (s.f.). Obtenido de https://criptotario.com/generaciones-de-blockchain-desde-bitcoin-a-muchos-mas
- *El tiempo*. (13 de Diciembre de 2016). Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/precio-del-bitcoin-en-2016-45452
- González, G. (Diciembre de 2018). *Criptonoticias*. Obtenido de https://www.criptonoticias.com/colecciones/altibajos-precio-bitcoin-historia/
- *I'MNOVATION #hub*. (s.f.). Obtenido de https://www.imnovation-hub.com/es/transformacion-digital/que-es-blockchain-y-como-funciona-esta-tecnologia/
- Mata, I. G. (14 de Marzo de 2018). *A Medium Corporation*. Obtenido de https://medium.com/@igmata/criptograf%C3%ADa-b%C3%A1sica-para-entender-la-tecnolog%C3%ADa-blockchain-eb94cdd64158
- *Miethereum*. (s.f.). Obtenido de https://miethereum.com/mineria/
- *Nocreasnada*. (s.f.). Obtenido de https://www.nocreasnada.com/como-funciona-blockchain/
- Ochoa, R. (5 de Julio de 2018). *El criptógrafo*. Obtenido de https://elcriptografo.com/2018/07/05/que-es-proof-of-work-entendiendo-blockchain/
- *OroyFinanzas* . (15 de Diciembre de 2014). Obtenido de https://www.oroyfinanzas.com/2014/12/que-es-bitcoin-days-destroyed-dias-bitcoins-destruidos/
- *P2P foundation*. (11 de Febrero de 2009). Recuperado el 25 de Marzo de 2019
- Pastor, J. (22 de Octubre de 2015). *Xakata*. Obtenido de https://www.xataka.com/empresas-y-economia/europa-dicta-sentencia-bitcoin-y-otras-monedas-virtuales-quedan-libres-de-impuestos

- Pastor, J. (1 de Marzo de 2019). *Xataka*. Obtenido de https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda
- Preukschat, A. (13 de Noviembre de 2013). *OroyFinanzas*. Obtenido de https://www.oroyfinanzas.com/2013/11/precio-bitcoin-cotizacion-2010-2011/
- Preukschat, A. (15 de Noviembre de 2013). *OroyFinanzas*. Obtenido de https://www.oroyfinanzas.com/2013/11/precio-del-bitcoin-en-2013-el-ano-del-bitcoin-con-precios-maximos-historicos/
- Preukschat, A. (18 de Enero de 2019). *Libro Blockchain*. Obtenido de https://libroblockchain.com/consenso/
- Preukschat, A. (18 de Enero de 2019). *Libro Blockchain*. Obtenido de https://libroblockchain.com/hashcash/
- Savedra, A. (20 de Marzo de 2018). *Criptodinero*. Obtenido de https://criptodinero.es/bitcoin/evolucion-del-precio-del-bitcoin-en-2017-2018/
- *Wikipedia*. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Peer-to-peer
- *Xataka*. (11 de Diciembre de 2017). Obtenido de https://www.xataka.com/criptomonedas/el-numero-de-bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

DEPÓSITO DEL TRABAJO FIN DE GRADO

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DEL TRABAJO FIN DE GRADO

Considerando que la presentación de un trabajo hecho por otra persona o la copia de textos, fotos y gráficos sin citar su procedencia se considera plagio,

Yo, ~~Don~~/Dña. ....ELENA....MARTÍNEZ....SALAS....., con DNI ..30262727X.....

estudiante del Grado en .ADMINISTRACIÓN..Y..DIRECCIÓN..DE..EMPRESAS..... de la

FCA....DE..CIENCIAS..ECONÓMICAS..Y..EMPRESARIALES..... de la Universidad de Sevilla, **ASUMO LA AUTORÍA RESPONSABLE Y DECLARO** que el Trabajo de Fin de Grado que presento para su exposición y defensa titulado ...TECNOLOGÍA..DEL..BLOCKCHAIN..Y..SU..APLICACIÓN..A..LA..EVOLUCIÓN..Y..PERSPECTIVAS..DEL..BITCOIN y cuyo tutor es D../Dña.....FRANCISCO....BARBERO...CUESADA.....

ES ORIGINAL Y QUE TODAS LAS FUENTES UTILIZADAS PARA SU REALIZACIÓN HAN SIDO DEBIDAMENTE CITADAS EN EL MISMO.

Así mismo, acepto que el profesorado podrá utilizar las herramientas de control del plagio que garanticen la autoría de este Trabajo de Fin de Grado.

Sevilla, a ..27..de .....MAYO..... de 2019

Firmado: ELENA MARTÍNEZ SALAS