Universitat Oberta de Catalunya

uoc.edu

Estudio de tecnologías Bitcoin y Blockchain

Benito López Rodríguez
TFM – Ad hoc

Consultora: **Ángela María García Valdés**

Resumen

La crisis económica de 2008, junto con la integración financiera en Europa y el desarrollo de nuevas tecnologías digitales provocó el nacimiento en 2009 de la criptomoneda Bitcoin, una alternativa al sistema monetario tradicional.

Bitcoin surge entonces con el objetivo de que dos usuarios realicen entre ellos transacciones monetarias a nivel mundial basándose en pruebas criptográficas en vez del sistema de confianza de organismos pertenecientes al sistema monetario tradicional como son Gobiernos o entidades bancarias.

La criptomoneda Bitcoin opera sobre la tecnología de código abierto denominada Blockchain (cadena de bloques). Este sistema se trata de una base de datos distribuida en ordenadores mediante red P2P, y en la que se almacenan en bloques todas las transacciones por orden cronológico que conforman una cadena de operación contable entre pares.

En este TFM se estudian los elementos y características de la tecnología Blockchain sobre la criptomoneda Bitcoin. Se explicarán sus ventajas y desventajas, sus diferencias con el modelo de transacción tradicional y su uso en aplicaciones potenciales actuales y futuras, desarrollando el estudio sobre su uso en Smart Contracts (contratos inteligentes).

Por último, se analizarán otros Blockchains actuales, la problemática de su regularización, su impacto en mercados financieros globales y la continuidad en el futuro de este tipo de monedas.

Summary

The economic crisis of 2008, together with the financial integration in Europe and the development of new digital technologies, led to the birth of Bitcoin cryptocurrency in 2009, an alternative to the traditional financial system

Bitcoin then arises with the aim that two users make financial transactions between them based on cryptographic tests instead of the trust system of organizations belonging to the traditional financial system such as governments or banking entities.

Bitcoin cryptocurrency operates on open-code technology called Blockchain. This system is a database distributed in computers through P2P network, and in which all transactions are stored in blocks in chronological order that make up a chain of transaction between peers.

In this “TFM” we study the elements and characteristics of the Blockchain technology on Bitcoin cryptocurrency. Its advantages and disadvantages will be explained, its differences with the traditional financial model and its use in current and future potential applications, developing the study on its use in Smart Contracts.

Finally, other current Blockchains will be analyzed, the problems of their regularization, their impact on global financial markets and the future continuity of this type of currencies.

Índice

1. Introducción 1

1.1 Objetivos 1
1.2 Metodología 2
1.3 Planificación 3
1.4 Estructura de la memoria 4

2. Bitcoin 5

2.1 Origen de Bitcoin 5
2.2 Características de Bitcoin 6
2.3 Arquitectura y organización de Bitcoin 8
2.4 Red P2P Bitcoin 9
2.5 Esquema de transacción en Bitcoin 10
2.6 Ventajas y desventajas de BitCoin 12
2.7 Impacto en los mercados 13

3. Blockchain 15

3.1 Definición 15
3.2 Arquitectura 16
3.3 Mecanismos de consenso 18
3.4 Blockchain público y privado 19

4. Aplicativos de Blockchain 20

4.1 Aplicaciones actuales 20
4.1.1 Criptomonedas 20
4.1.2 Navegadores 21
4.1.3 Almacenamiento 21
4.1.4 Donaciones 22
4.1.5 Registros médicos 22
4.1.6 Registros académicos 23
4.1.7 Comercio on-line 23
4.1.8 Informática colaborativa 23

4.2 Smart Contracts 24
4.2.1 Funcionamiento 25
4.2.2 Aplicaciones 26

4.3 Futuros aplicativos de Blockchain 27

5. Otras criptodivisas 29

5.1 Panorama actual 29
5.1.1 Etherum (ETH) 29
5.1.2 Bitcoin cash 29
5.1.3 Ripple (XRP) 30
5.1.4 Litecoin (LTC) 30
5.1.5 Cuadro comparativo 31

5.2 Regularización 31
5.3 Futuro en los mercados financieros 33

6. Conclusiones 34
7. Bibliografía 35

Lista de figuras

Figura 1: Planificación del proyecto 3

Figura 2: Anuncio de criptomoneda bitcoin por Satoshi Nakamoto..... 5

Figura 3: Ataque de doble gasto en Bitcoin..... 9

Figura 4: Transacción con bitcoins..... 10

Figura 5: bitcoins en circulación ($)..... 13

Figura 6: Volumen de intercambio comercial bitcoin..... 14

Figura 7: Precio bitcoin ($) 14

Figura 8: Bloque Blockchain..... 16

Figura 9: Vista simplificada de una cadena de bloques 17

Figura 10: Funcionamiento Smart Contracts..... 25

Lista de tablas

Tabla 1: Tabla comparativa de las principales criptomonedas 31

1. Introducción

Este TFM analiza la moneda criptográfica bitcoin desde el punto de vista técnico. funcional, y financiero.

El documento comenzará con una breve reseña histórica y un repaso de las características de esta criptomoneda más mediática y usada a día de hoy, atendiendo al protocolo de incentivos para consensuar transacciones, la seguridad de la arquitectura Bitcoin sobre tecnología Blockchian y su escalabilidad y transparencia para diferentes aplicativos.

Seguidamente se estudiará el protocolo Blockchain independientemente de bitcoin, para comprender la tecnología que crea una cadena de bloques de transacciones totalmente inmutable e integra

Por último, se citarán diferentes aplicativos actuales sobre Blockchain, desarrollando los Smart Contracts y otras criptomonedas alternativas al bitcoin.

1.1 Objetivos

El enfoque global del proyecto es el estudio de las tecnologías Bitcoin y Blockchain para comprender los beneficios genera esta tecnología en aplicaciones presentes y futuras. Para ello se cumplirán estos objetivos:

- Explicar la arquitectura y organización de la red Bitcoin.
- Explicar las ventajas del modelo peer-to-peer en comparación con el modelo de transacción tradicional.
- Explicar los conceptos de transacción, bloque y cadena de bloques
- Explicar los diferentes mecanismos de consenso de Blockchain, sus ventajas y desventajas.
- Explicar las diferencias entre Blockchain público y privado.
- Explicar aplicaciones actuales y futuras de la tecnología Blockchain
- Explicar el concepto de Smart Contracts.
- Introducir otros Blockchains actuales (por ejemplo, Ethereum, Ripple, Litcoin…).

1.2 Metodología

Las tareas a seguir para finalizar con éxito este estudio de tecnologías Bitcoin y Blockchain, se pueden separar en 5 bloques bien definidos que se abordaran en el siguiente orden:

1. Estudiar el nacimiento y arquitectura de la criptomoneda bitcoin.
    - Transacción, bloque y cadena de bloques.
    - Red P2P para bitcoin.
    - Consenso de Blockchain.
    - Blockchain publico/privado.

2. Estudio del algoritmo criptográfico Blockchain.
    - Arquitectura.
    - Criptografia asimétrica.
    - Generación de direcciones y clases privadas.

3. Estudio de aplicativos de Blockchain.
    - Aplicaciones actuales.
    - Aplicaciones futuras.
    - Futuro del Bitcoin.

4. Estudio de Smart Contracts
    - Funcionamiento.
    - Aplicaciones.

5. Critptodivisas alternativas.
    - Panorama actual
    - Regularización. Impacto en mercados financieros
    - Futuro

Dada la naturaleza del objeto del estudio, el principal recurso utilizado para el alcance de los objetivos descritos serán fuentes de internet.

1.3 Planificación

La duración estimada del estudio es de 85 días. El lanzamiento del proyecto comenzará el día 12 de Marzo de 2018, y se concentrará en 3 fechas clave:

- 9 de Abril de 2018 (PEC2): BitCoin y Blockchain
- 7 de Mayo de 2018 (PEC3): Aplicativos blocckChain + Smart Contracts
- 4 de Junio de 2018 (PEC4): Criptodovisas. Maquetación y entregables.

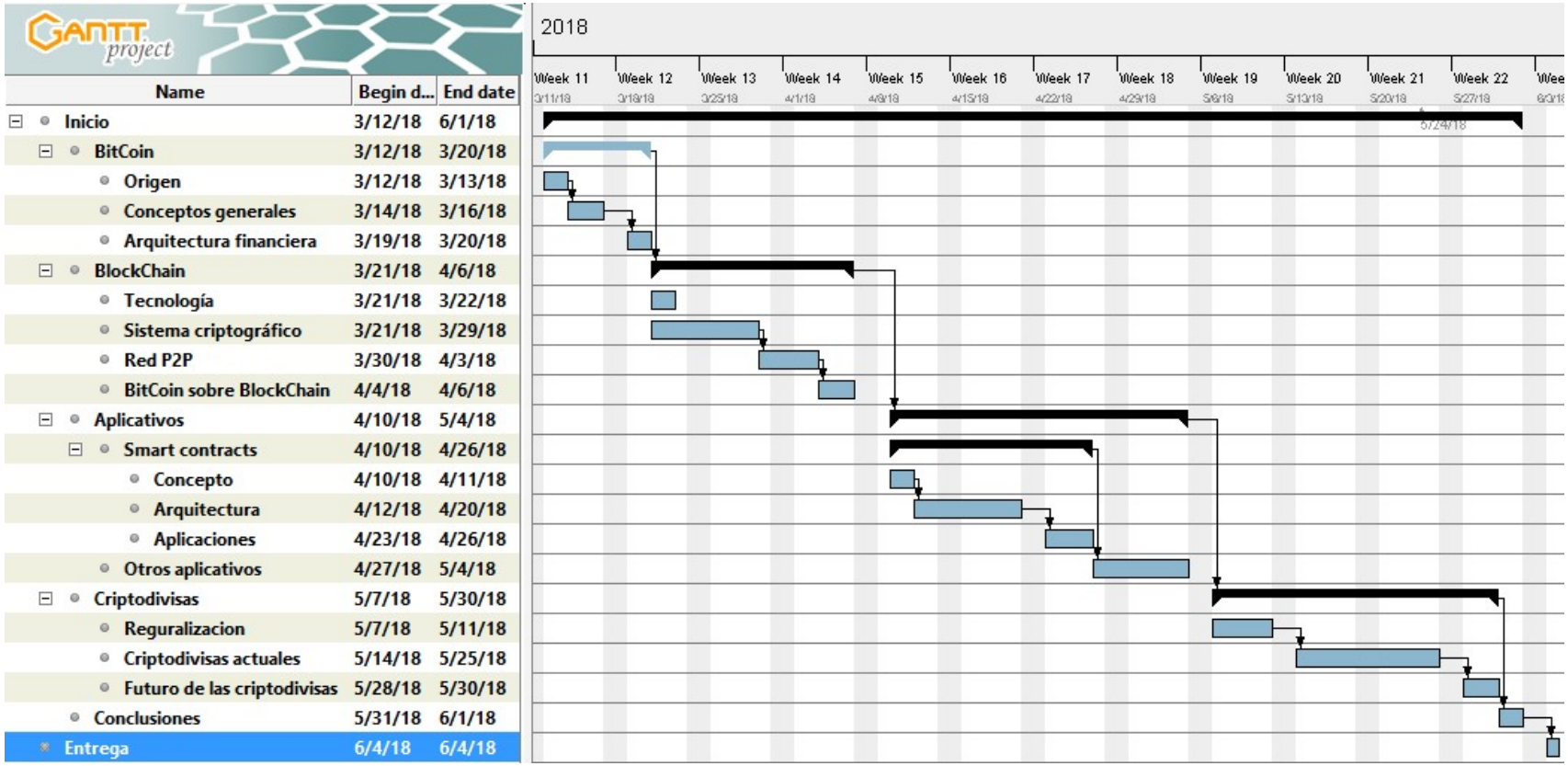


Figura 1: Planificación del proyecto

1.4 Estructura de la memoria

- **Bitcoin**:

  Se analiza el origen de la criptomoneda Bitcoin, las características más relevantes de ella, la arquitectura de todos los elementos que intervienen en la red Bitcoin. Además, se explica cómo funciona esta red Bitcoin mostrando un ejemplo de transacción. Por último, se indican las ventajas y desventajas significativas de Bitcoin y su impacto en los mercados.

- **Blockchain**:

  Se analiza la arquitectura de la tecnología Blockchain atendiendo a su organización y seguridad. Se describen los tipos de Blockchain y como se alcanza el consenso

- **Aplicativos**:

  Se describen aplicativos actuales de la tecnología Blockchain, y en concreto se analiza en profundidad los Smart Contracts. También se analiza el futuro de Blockchain en diferentes aplicativos.

- **Criptodivisas**:

  Se analiza la regularización de las criptodivisas, entre las que se estudian las 4 más importantes junto con Bitcoin: Etherim, Bitcoin cash, Ripple y Litecoin.

  Por último, se verá el impacto actual de las criptodivisas y su fututo en los mercados financieros

- **Conclusiones**.

- **Bibliografía**.

2. Bitcoin

2.1 Origen de Bitcoin

El concepto de moneda criptográfica fue descrito por primera vez en 1998 por Wei Dai en la lista de correo electrónico “cypherphunks”. Su definición sería un tipo de dinero que utilizaría la criptografía para ser creado y para controlar sus transacciones, en vez de lo que hiciera una autoridad gubernamental.

Sin embargo no fue hasta Noviembre de 2008, cuando motivado por la idea de Wei Dai, y la crisis financiera del aquel momento, un inventor o inventora anónimo que utilizaba el seudónimo “Satoshi Nakamoto” publicó un artículo científico (https://bitcoin.org/bitcoin.pdf) mediente Cryptography Mailing List, describiendo el protocolo que había desarrollado: BitCoin

Satoshi Nakamoto

CATEGORY: CRYPTOGRAPHY MAILING LIST

Bitcoin P2P e-cash paper

NOVEMBER 1, 2008 • SATOSHI NAKAMOTO • CRYPTOGRAPHY MAILING LIST

I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party. The paper is available at: http://www.bitcoin.org/bitcoin.pdf The main properties: Double-spending is prevented with a peer-to-peer network. No mint or other trusted parties. Participants can be anonymous. New coins are made from Hashcash style [...]

Figura 2: Anuncio de criptomondeda bitcoin por Satoshi Nakamoto

El 3 de enero de 2009 la red P2P de Bitcoin entra en funcionamiento con la publicación del primer programa cliente, de código abierto, y la creación de los primeros bitcoins.

A finales de 2010 “Satoshi Nakamoto” abandona el proyecto que él/ella mismo había creado sin revelar su identidad; sin embargo, la comunidad de bitcoin ha crecido exponencialmente desde entonces, así como los desarrolladores de dicho protocolo y de sus aplicativos.

2.2 Características de Bitcoin

A continuación, se indican las características más destacadas de la criptomoneda Bitcoin:

- **Origen anónimo**: Se desconoce qué persona o grupo de personas la creó.
- **Código abierto**: Su código fuente es accesible para todo el mundo.
- **Satoshi**: Mínima unidad divisible del bitcoin; equivale a 0,00000001 bitcoin
- **Funciona sobre Blockchain**: Para almacenar la asignación de Bitcoins y el histórico de compras y ventas realizadas con ellos, se utiliza una base de datos descentralizada sobre varios nodos comunicados en red P2P. Esta tecnología es llamada Blockchain.
- **Descentralizada**: Ningún organismo gubernamental o banco controla Bitcoin. Así no es posible generar inflación; solo la minería controla descentralizadamente -y en función de la demanda-, la emisión de Bitcoins.
- **≤ 21 millones**: Nunca se podrán exceder los 21 millones de bitcoins. Bitcoin se creó a modo de moneda deflacionaria, ya que, si es escasa de forma natural, tendrá más valor.
- **Infalsificable ni duplicable**: Mediante un potente sistema criptográfico se protege al dueño del Bitcoin para que tenga su monedero exclusivo con el que se gestiona sus Bitcoins, solo cuándo aquél lo desee.
- **No legislada**: Es una moneda sin ninguna regulación. Por ello no existe organismo que proteja al consumidor ni ley donde ampararse ante problemas en transacciones.
- **Volátil**: Bitcoin no depende de ningún mercado, por lo que sufre alzas y bajas en su valor frecuentemente. Por la naturaleza de Bitcoin, su seguridad y por extensión la confianza en esta criptodivisa es una de las razones de su fluctuación.
- **Permutable**: Las unidades de Bitcoin son intercambiables.
- **Intercambiable:** Se pueden cambiar bitcoins por otras divisas y viceversa.
- **Pertenece al 100% del usuario** en todo caso, de forma que sus bitcoins no pueden ser intervenidos ni se pueden congelar sus cuentas asociadas.
- **Sin permiso**: La participación en la red Bitcoin no está arbitrada.

- **Pseudoanónima**: La red de Bitcoin no requiere identificarse para participar en ella. Sí se conocen las claves públicas utilizadas en las transacciones, mientras que los usuarios son responsables del resguardo de las claves privadas utilizadas en dichas transacciones.

- **Sin censura**: Nadie puede prohibir transacciones válidas.

- **Sin intermediarios:** Las transacciones son directas entre personas, y al basarse en una red P2P, casi instantáneas.

- **Transacciones irreversibles:** No es posible modificar ni anular transacciones confirmadas. Cierto es que se han desarrollado aplicativos cómo “ESCROW” para garantizar el acuerdo entre usuarios por un periodo de tiempo.

2.3 Arquitectura y organización de Bitcoin

Para describir la arquitectura de funcionamiento de Bitcoin, se describen los actores que intervienen en el conjunto del protocolo:

- **bitcoin / shatoshi:** bitcoin es la unidad de la criptodivisa, mientras que shatoshi es la mínima unidad de pago, que equivale a la cienmillonésima parte de un bitcoin.

- **Usuario de BitCoin:** Puede ser cualquier persona o entidad. Para ser usuario de Bitcoin en primer lugar es necesario registrase en la red Bitcoin obteniendo una dirección Bitcoin. Para ello lo más común es comprar bitcoins en casas de cambio especializadas.

- **Casas de cambio:** Son empresas que disponen de aplicaciones para comprar y vender Bitcoins de forma sencilla, cobrando una pequeña comisión. Bitstamp.net, Kraken.com, Coinbase.com o Xapo.com son algunas de las empresas que pueden almacenar bitcoins, aunque se recomienda siempre utilizar un monedero propio.

- **Monedero:** Es un espacio virtual dónde se almacenan las direcciones de Bitcoin de un usuario, así como las transacciones realizadas con ellas.

- **Dirección Bitcoin:** Al igual que una cuenta bancaria, una dirección Bitcoin es una dirección virtual de un usuario de la red BitCoin. Esta dirección se identifica con una clave pública, representada por cifras y letras.

- **Clave pública**: Identifica la dirección de Bitcoin y se utiliza para validar las firmas de las transacciones realizadas en esta red.

- **Clave privada:** Es la prueba de identidad, que debe ser solo conocida por el dueño de los Bitcoins asociados

- **Transacción:** Transferencia de dinero entre dos direcciones de Bitcoin.

- **Bloque:** Almacena transacciones pendientes de confirmar que serán validadas mediante el proceso de minería.

- **Minería:** Es el proceso por el que mineros (potentes ordenadores) realizan complicados cálculos matemáticos para confirmar las transacciones pendientes de validar que estaban almacenadas en los bloques. Tras confirmar una transacción, el minero la almacena en las cadenas de bloques cronológicamente, y recibe una remuneración en bitcoins por ello

- **Consenso:** Las transacciones en bitcoin son validadas por usuarios de la red Bitcoin mediante un algoritmo de consenso distribuido basando en prueba de trabajo.

- **Cadena de Bloques:** Se trata de un registro público de las transacciones con Bitcoins confirmadas por los mineros.

2.4 Red P2P Bitcoin

Las redes P2P (peer-to-peer) están formadas por nodos que se comportan como iguales entre sí, de forma que realizan funciones de cliente y servidor con el resto de nodos, con los que comparten información. El protocolo Bitcoin basa su comunicación entre nodos sobre red P2P por estas razones:

- Escalabilidad: Se basa en código abierto, lo que permite flexibilidad, y un alcance mundial a cualquier dispositivo conectado a internet. Además, cuantos más nodos Bitcoin, más recursos compartidos que mejoran el rendimiento del sistema global.
- Robusto: La información está en todos los nodos (ninguno imprescindible).
- Descentralización: No se realizan peticiones a un único servidor central.
- Distribución de costes: Se utilizan los recursos de todos los nodos (ancho de banda, almacenamiento, ciclos de proceso) para un bien común.

Para ser un nodo Bitcoin e incorporarse a su red P2P, se debe descargar e instalar el software “Bircoin core” junto con el archivo de cadena de bloques “bootstrap.dat” (libro de contabilidad de “Blockchain”), cuyo tamaño actual de 200Gb almacena desde la primera transacción en 2009 hasta la más actual.

Así, cada que vez que se realiza una transacción y se actualiza la cadena de bloques, todos los nodos de red Bitcoin utilizan el protocolo Bitcoin sobre la red P2P para actualizar este libro de contabilidad, manteniendo así un registro de contabilidad descentralizado.

El protocolo Bitcoin sobre la arquitectura P2P resuelve el problema de doble gasto que existía en intercambio de digital de dinero sin confirmación, y por el cual un comprador actuando de mala fe, podría realizar dos compras simultáneas usando el mismo dinero.

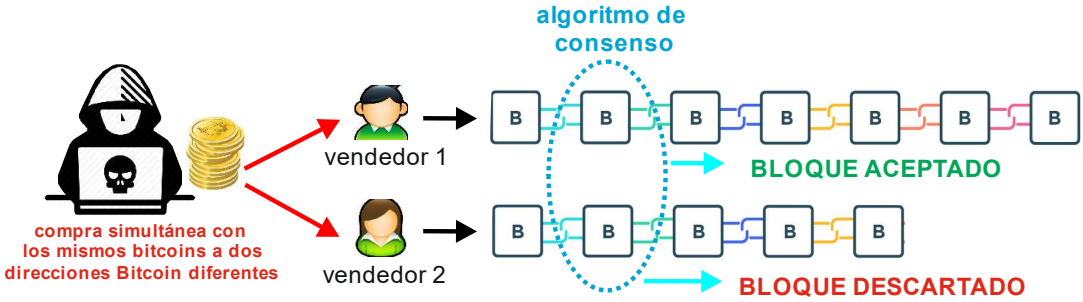


Figura 3: Ataque de doble gasto en Bitcoin

Esto es porque en una red Bitcoin, un minero deberá resolver mediante un mecanismo de consenso cuál de las dos transacciones se procesará, añadiendo la transacción verificada a un bloque, con lo que se elimina el problema de doble gasto (a día de hoy no se ha conseguido copiar una unidad de bitcoin, ni corromper la red P2P para crear bitcoins unilateralmente)

2.5 Esquema de transacción en Bitcoin

A continuación, se muestra una imagen del circuito a seguir para realizar una transacción con bitcoins, describiendo los pasos de que consta:

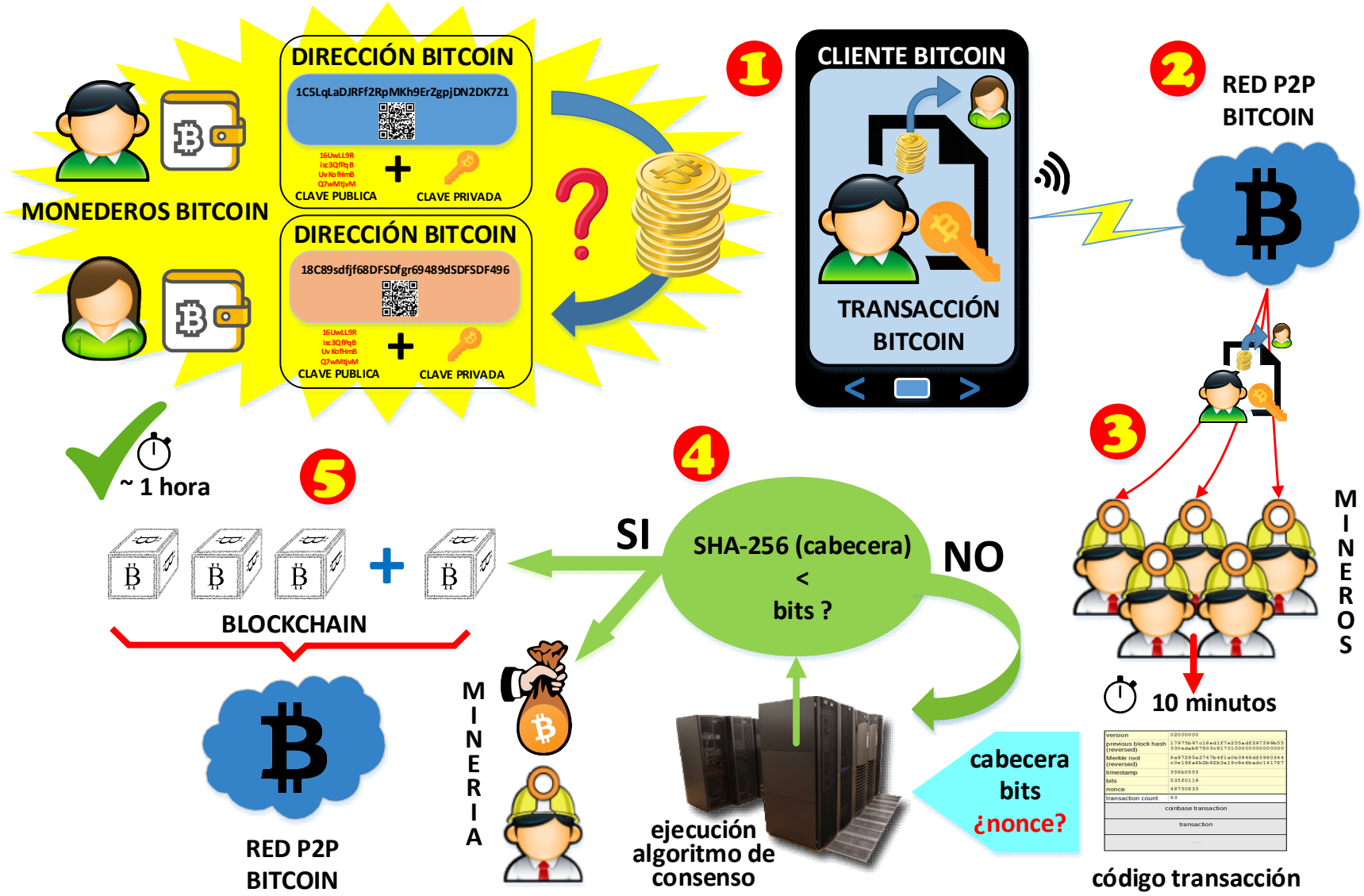


Figura 4: Transacción con bitcoins

Descripción de ejemplo de transacción:

0. Los usuarios de Bitcoin A y B quieren realizar una transferencia de bitcoins entre ellos. Cada uno tiene su propio monedero Bitcoin que contendrá direcciones de Bitcoin, y que usan para realizar sus gestiones. Cada dirección de Bitcoin es un par de claves pública y privada, identificada con el hash de la clave pública más una suma de verificación. La clave privada la sabrán únicamente sus dueños, y la utilizarán para firmar sus transacciones. En este caso el usuario A utilizará la dirección de Bitcoin "1C5LqLaDJRFf2RpMKh9ErZgpjDN2DK7Z1" de su monedero Bitcoin para transferir bitcoins a la dirección Bitcoin "18C89sdfjf68DFSDfgr69489dSDFSDF496" perteneciente al usuario B.

1. Para iniciar la transacción, el usuario A utiliza el cliente de Bitcoin instalado en su dispositivo, y crea una transacción, formada por entradas y salidas: Las entradas serán registros que referencian fondos de transacciones previas, y las salidas serán los registros que referencian al nuevo propietario y a la dirección del pagador para recibir la vuelta. No es necesario indicar el valor en bitcoins de la operación, porque se trasfieren todos los fondos de la dirección de Bitcoin entrada a la de salida indicados. Para finalizar la creación de transacción, el usuario A la firma con su clave privada de su dirección Bitcoin, desbloqueando los fondos de la dirección.

2. La transacción creada es enviada a la red P2P de Bitcoin, en donde los usuarios A y B son identificados únicamente por sus claves públicas. Cada nueva transacción se agrupa periódicamente en un bloque de transacciones recientes.

3. Los mineros de Bitcoin son alertados de que existe una nueva transacción a validar. Pasados 10 minutos recogen la transacción, convirtiéndola en un nuevo código de transacción para poder ser tratada:

4. El minero inicia un proceso computacionalmente intensivo llamado mecanismo de consenso que tiene por objeto hallar una prueba de trabajo ("Proof of Work") en forma de código aleatorio cuyo nombre es nonce (number used only once), y que debe satisfacer este requisito criptográfico: Nonce debe ser un hash SHA-256 de los campos cabecera del bloque de transacción, y cuyo valor será menor que el del campo bits.

5. El bloque ha sido validado. El minero añade el bloque a la cadena de bloques e ingresa en su monedero la recompensa por haber resuelto la prueba criptográfica. Se le comunica la validación del nuevo bloque al resto de nodos para que actualicen su base de datos.

   A fin de dar tiempo a los nodos a que verifiquen que un nuevo bloque es correcto, -por si surgen dos ramas distintas inicialmente válidas- entre los bloques confirmados por diferentes mineros, se establece un tiempo de 6 bloques (6 bloques validados desde la transacción) hasta dar por válida la transacción. Cómo el tiempo medio de generación de un bloque es cada 10 minutos, una transacción se considera confirmada la hora de realizarse.

2.6 Ventajas y desventajas de bitcoin

Las transacciones mediante bitcoin resuelven algunos defectos de las transacciones tradicionales; sin embargo, existen problemas asociados a la naturaleza de la criptomoneda que no se pueden obviar:

VENTAJAS:

- Tecnológicas

  - ✓ Disponibilidad: base de datos descentralizada y distribuida.
  - ✓ Seguridad: bloques de transacciones íntegros, inmutables.
  - ✓ Privacidad: sistema criptográfico asegura el patrimonio de bitcoins sin necesidad de identificarse.

- Financieras

  - ✓ Global: no pertenece a ningún banco o gobierno.
  - ✓ Independiente del sistema fiduciario. No puede ser intervenido.
  - ✓ Barato: no hay comisiones en las transacciones.
  - ✓ Transparente: Toda transacción registrada y de libre acceso.
  - ✓ No falsificable.
  - ✓ Rapidez en las transacciones (máximo 10 minutos de ejecución).
  - ✓ Funciona en cualquier momento, las 24 horas del día.
  - ✓ Su moneda divisible hasta 10^{-8} (satoshi), beneficia micropagos.
  - ✓ El anonimato beneficia su uso en regímenes totalitarios.

DESVENTAJAS:

- Tecnológicas

  - ✓ El tamaño de la base de datos crece exponencialmente.
  - ✓ Velocidad de transacción lenta (7 transacciones por segundo).
  - ✓ Su algoritmo de consenso provoca un alto consumo de energía.

- Financieras

  - ✓ No se permite la adquisición de cualquier bien.
  - ✓ No todos los comercios aceptan bitcoins.
  - ✓ La ausencia de regulador puede incomodar los mercados.
  - ✓ El cambio con las monedas tradicionales es muy volátil, siendo éstas las que marcan los precios de servicios y bienes.
  - ✓ Su límite de emisión (21 millones) puede deprimir la economía.
  - ✓ El anonimato puede provocar actividades ilícitas.

2.7 Impacto en los mercados

La criptomoneda bitcoin surgió tras la crisis financiera de año 2009 como alternativa de las monedas tradicionales devaluadas por dicha crisis, y con el objetivo de salvaguardar el capital sin verse afectado por estas situaciones, en las cuales un organismo público regula la actividad monetaria.

Si bien desde un punto de vista contable, los bitcoins son bienes digitales y no activos financieros, su adquisición incrementa el patrimonio, y actualmente se mantiene el pulso entre la moneda tradicional y criptomoneda, creciendo la actividad exponencialmente de esta última debido a una razón principal: se realizan transacciones de forma ágil y directamente entre comprador y vendedor sin las comisiones ni regulaciones impuestas por un banco.

De esta forma, son cada vez más los nodos Bitcoin, las empresas que incluyen bitcoins como método de pago, e incluso las empresas que pagan el salario a sus trabajadores con dicha criptomoneda, por lo que se puede afirmar que los mercados promueven el uso de bitcoin y su establecimiento es cada vez más firme.

A fecha de hoy circulan 17 millones de bitcoins en el mercado (fig. 5), con un volumen de 173.000 transacciones diarias (fig. 6), y una tasa de cambio bitcoin-dolar que supera los 500 millones de dólares diarios.

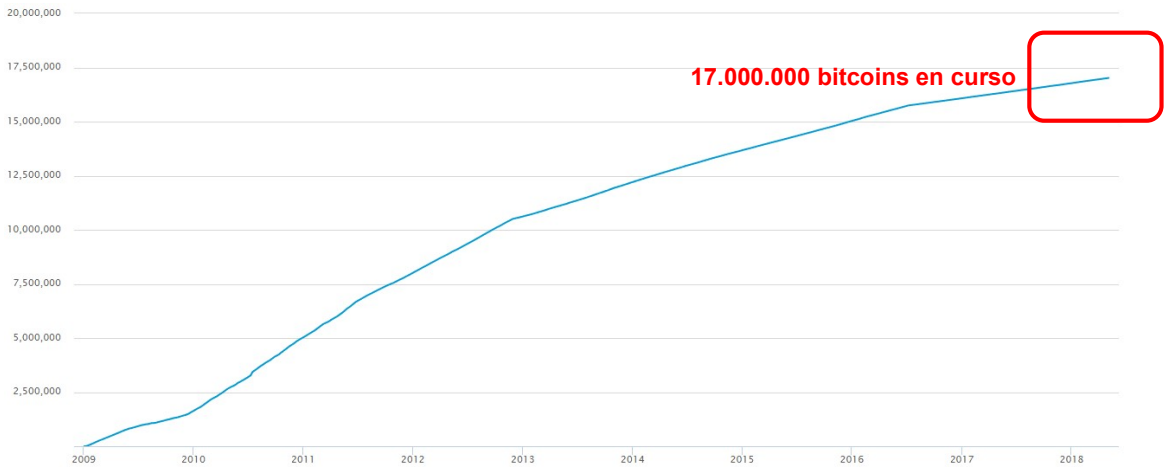


Figura 5: bitcoins en circulación ($)

Según este crecimiento de la masa monetaria de bitcoins , se prevé alcanzar el límite de 21 millones de bitcoins en curso en el año 2040.

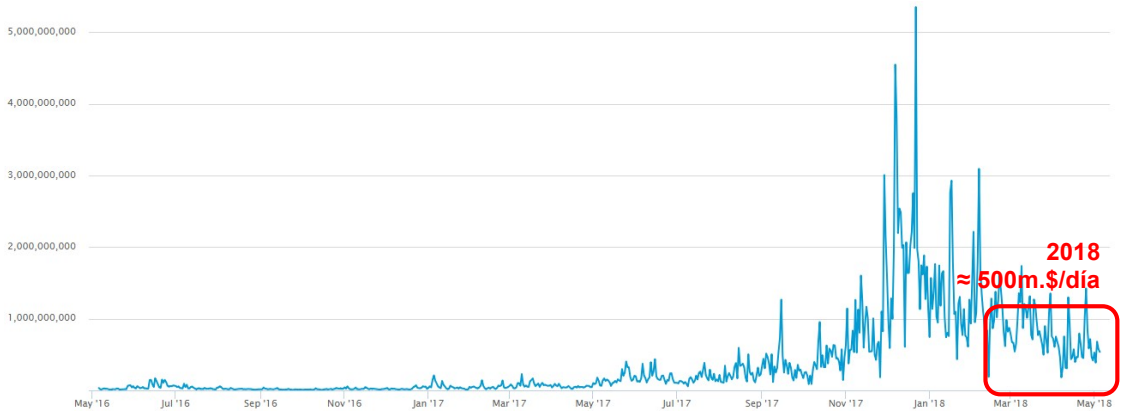


Figura 6: Volumen de intercambio comercial bitcoin/$

Si bien, en el último año 2017 se ha comprobado la enorme volatilidad de bitcoin. Esto se puede comprobar en el siguiente gráfico, dónde se observa cómo desde su nacimiento en 2009 tuvo un valor muy pequeño hasta 2014 cuando subió hasta 800$ manteniéndose así durante tres años y siendo 2007 el año en que estuvo en alza hasta tener un valor máximo histórico de 17.549,17$ en diciembre de 2017 y bajando hasta su valor actual de 7.000$ aproximadamente:

Figura 7: Precio bitcoin ($)

Los datos sobre bitcoin son dinámicos; cambian a cada instante. Muchas son las webs que hacen eco de todos estos valores con fines financieros, como la web http://bitcoin.com o http://Blockchain.info que indican en todo momento el valor del bitcoin en dólares, las transacciones diarias, o el número de bitcoins en curso, entre otros valores interesantes.

3. Blockchain

3.1 Definición.

Como se ha visto en el apartado anterior, bitcoin utiliza su red P2P para mantener su actividad. Ello es posible a la tecnología Blockchain mediante la cual se implementa la base de datos distribuida, segura y formada por las transacciones consensuadas entre nodos Bitcoin.

Blockchain es un libro de contabilidad formado por registros (bloques) enlazados y cifrados para poder proteger la privacidad y seguridad de su actividad.

Se eliminan intermediarios, pero las transacciones deben ser validadas igualmente. Para ello, en la red P2P existen nodos llamados “mineros” que reciben alertas de nuevas transacciones para agregar a un bloque.

Con bitcoins sobre Blockchain, los mineros competirán entre ellos para validar (resolviendo un problema criptográfico), sellar y recibir una recompensa en bitcoins por el servicio prestado. El mecanismo de consenso “Proof of work” utilizado por el minero de bitcons será el corazón de Blockchain, para mantener la integridad de la información.

Las características principales de la tecnología Blockchain son:

- Mecanismo de consenso: es el base de Blockchain, por la que los nodos utilizan un sistema para actualizar la información de forma consensuada.

- Seguridad: Por diseño, una vez añadido un bloque de transacciones a la cadena, éste no se puede modificar, solo consultarse, asegurando así su inmutabilidad e integridad.

- Confiable: la arquitectura de nodos igual a igual distribuidos sobre la red de trabajo P2P, hace confiable la información por su descentralización, disponibilidad y escalabilidad.

- Transparencia y trazabilidad: la arquitectura de la tecnología asegura la limpieza de los registros, creados por el propio protocolo, siendo auditables en cualquier momento.

- Ahorro de costes y tiempo: Por la arquitectura de la cadena de bloques, se reducen las tareas de registro y control en los datos de las transacciones.

- Agilidad: las transacciones son en tiempo real: sin demoras por auditorías de organismos externos.

3.2 Arquitectura.

Para comprender la arquitectura de funcionamiento de Blockchain, es necesario estudiar el contenido de uno de sus bloques. A continuación, se muestra la estructura lógica de un bloque de Blockchain:

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Figura 8: Bloque Blockchain

- <u>version (16 bits)</u>: indica la versión del protocolo Blockchain que ha utilizado el minero del bloque.

- <u>previous block hash (128 bits)</u>: contiene el hash del bloque anterior con el que esta enlazado en la cadena Blockchain, para establecer la secuencia temporal y asegurar la consistencia en la cadena de bloques.

- <u>merkle root (128 bits)</u>: contiene el hash del bloque actual con el que se verifica que el contenido de transacciones no ha sido modificado tras validarlo y añadirse a la cadena de Blockchain.

- <u>timestamp (16 bits)</u>: fecha y hora en formato “timestamp” del minado del bloque.

- <u>bits (16 bits)</u>: representa un valor de 128 bits (calculado a partir de una mantisa -byte 3- y un exponente -bytes 0,1,2-), que indica el límite del hash del bloque. Es el que marca la dificultad de computación en el minado del bloque, de forma que el minero debe hallar un valor en el campo “nonce” (siguiente campo de la cabecera) que, aplicado al bloque, y realizando hash SHA-256 de éste, el valor resultante debe ser menor a este campo “bits”.

- nonce (16 bits): contiene la prueba de trabajo según el mecanismo de consenso seleccionado. Como se ha indicado en el campo anterior, representa el conjunto de bytes calculados por el minero que hacen cumplir los criterios de dificultad marcados por el campo “bits” y el propio bloque.

Hasta aquí finalizan los campos de la cabecera del bloque de Blockchain, y empieza el cuerpo del bloque formado por el número de transacciones que contiene, seguido de todas ellas.

- transaction count (longitud variable): indica el número de transacciones del bloque.

- Transaction: es el cuerpo de la transacción en sí, que indica origen, destino, firma de la transacción y número de satoshis (en caso de transacción bitcoin) entre otros.

A continuación, se muestra una vista simplificada de una cadena de bloques:

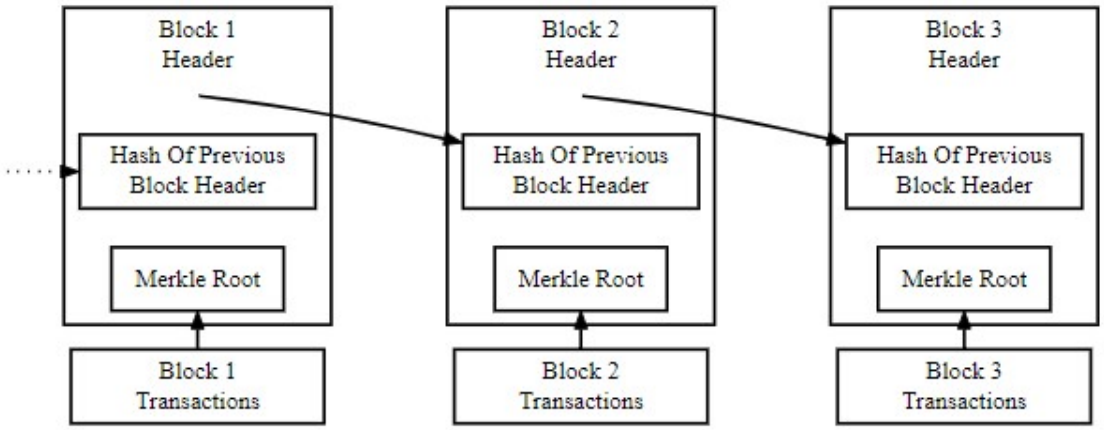


Figura 9: Vista simplificada de una cadena de bloques

Cada bloque está formado por una o varias transacciones que se almacenan en el campo “transaction data” del cuerpo del bloque. A cada una de estas transacciones se le calcula su hash, y se van emparejando con el resto de hashes de cada transacción, hasta que quede un solo hash, que será el “merkle root” del bloque.

Este valor de hash “merkle root” se almacena en cada bloque, y en cada bloque también se almacenará el hash de la cabecera del bloque anterior, encadenándose así los bloques como muestra la figura 9, y garantizando la inmutabilidad de los bloques y su información.

3.3 Mecanismos de consenso

El mecanismo des consenso de Blockchain es el sistema que controla de qué forma se añaden nuevos bloques verificados a la cadena de Blockchain. Se debe asegurar la integridad de toda la información de la base de datos de blocjkChain y detectar anomalías. Para ello, Blockchain se basa en la teoría de juegos y en el equilibrio de Nash, por las que se crearan unas reglas de consenso en forma de pruebas criptográficas para que los mineros que las realicen dispongan de incentivos por los cuales les compense actuar de forma honesta, maximizando su rentabilidad y logrando una cadena de bloques legítima.

Con Blockchain el consenso descentralizado requiere la aceptación de los nodos de la red, para la cual se utilizan protocolos. Estos protocolos son los algoritmos de consenso, de los cuales existen varios:

- Proof of work (prueba de trabajo):

  Es el algoritmo que utilizan las criptomonedas Bitcoin y Etherum. Se basa en el algoritmo hashcash, por el cual se exige al usuario incurrir en un coste para poder realizar una función. En este caso el coste es capacidad de computo, por el cual un minero es recompensado tras realizar una compleja prueba criptográfica. Tras finalizar la tarea, el minero es recompensado por el sistema. En el apartado 2.4 se describe este mecanismo de consenso.

- Proof of stake (prueba de participación):

  El algoritmo utilizado hace que en vez de crear bloques en proporción a la capacidad de computo como es el caso de Proof of Work, los bloques se crean en proporciona a la cantidad de tokens que disponga el minero recompensándolo mediante comisiones por transacción.

  Para asignar los bloques a los mineros existen dos métodos:

  - ✓ Selección aleatoria: El minado de cada bloque se asigna a cualquiera se los tokens existentes. Esto incentiva a tener los sistemas online a quien tenga más tokens.

  - ✓ Selección por antigüedad de moneda: Se asigna el bloque a quien halla realizado una transacción con criptomonedas que tengan más tiempo desde la última vez transferidas.

  Este algoritmo es más rápido y requiere menos consumo de energía que Proof of Work.

3.4 Blockchain público y privado

Blockchain nació con bitcoin de la mano de la entidad “Satoshi Nakamoto”; sin embargo, la tecnología Blockchain es muy potente y ya se aplica a diferentes ámbitos, surgiendo nuevas formas de trabajar con él.

Hablar de Blockchain público o privado, es similar a hablar cadenas de bloques sin permiso (permissionless Blockchain), o con permiso (permissioned Blockchain):

- **Blockchain público**

  La cadena de bloques de bitcoin es un Blockchain público, al igual que otras criptomondeas como Ethereum, Litecoin o Namecoin. Así un Blockchain público se caracteriza por:

  - ✓ Cualquier persona puede mantener la base de datos.
  - ✓ Cualquier persona puede acceder a la base de datos.
  - ✓ Cualquier persona puede realizar transacciones, las cuales se registrarán en la base de datos.
  - ✓ La base de datos es distribuida masivamente.
  - ✓ El incentivo para mantener la base de datos es económico-criptográfico. Se recompensa económicamente por una labor criptográfica, como se verá en el apartado 3.3.

- **Blockchain privado**

  Las cadenas de bloques privadas son aquellas en las que los participantes que la forman y el proceso de consenso están limitados. Así, un Blockchain privado se caracteriza por:

  - ✓ Una entidad o grupo de entidades mantienen la base de datos.
  - ✓ Solo las entidades preseleccionadas pueden acceder a la base de datos, y se puede delimitar los derechos a partes de ésta.
  - ✓ Solo las entidades con permiso pueden realizar transacciones que se registraran en la base de datos.
  - ✓ La base de datos está centralizada o almacenada en entidades preseleccionadas.
  - ✓ La base de datos se mantiene por un interés propio.

- **Blockchain híbrido**

  Se trata de una combinación de las dos anteriores, dónde los nodos participantes son seleccionados, pero las transacciones son públicas. Los nodos participantes mantienen la seguridad del Blockchain pero al ser visibles las transacciones para todos los nodos, se facilita la gestión de la Identidad Digital Soberana.

4. Aplicativos de Blockchain

En este apartado del TFM se van a desarrollar otros usos de la Blockchain no relacionados con los bitcoins. Además, se analizarán los Smart Contract, que surgen del pago en criptomonedas, y se establecerán distintas sugerencias sobre el uso futuro de la Blockchain.

4.1. Aplicaciones actuales

4.1.1. Criptomonedas

El uso más común y conocido de la Blockchain es el relacionado con las criptomonedas, en concreto con bitcoin. Según Valentín Pich, presidente del Consejo General de Economistas de España, la Blockchain es una herramienta que fundamentalmente permite el ahorro de costes de documentación en los procesos de gestión de los bancos y que destaca por su fiabilidad, ya que las transacciones quedan consignadas fehacientemente y registradas de forma inalterable.

Así pues, utilizar la tecnología Blockchain en el sistema bancario y financiero permitirá que no se puedan modificar a posteriori datos sobre transacciones y movimientos de cuentas bancarias. Esto es fundamental para luchar contra el fraude, ya que podrá rastrear sin ningún género de duda los movimientos bancarios de las cuentas. Sin embargo, para que este uso sea real y posible, es necesario que exista una colaboración plena de las entidades financieras, no solo a nivel local, sino a nivel mundial. En este aspecto, los bancos centrales de los distintos países podrían ser una herramienta esencial y sin cuya plena implicación sería inviable aplicar la tecnología Blockchain al entramado financiero.

En este uso de la Blockchain en el espectro financiero se produce un impedimento más: su aplicación en los sistemas de financiación privado que han aflorado al margen de la banca tradicional. Son más opacos, tienen sus propias reglas y detrás de ellas se encuentran inversores privados.

Además de este uso, la Blockchain ofrece otras ventajas en diversos ámbitos y es lo que se va a desarrollar en este apartado:

4.1.2. Navegadores

Encontramos aquí al navegador **Blockstack**. Es un navegador especial y orientado a la ejecución de aplicaciones que están descentralizadas o distribuidas a través de una red encriptada. Hay que indicar que en sí no es un navegador, sino una aplicación que permite la navegación dentro de otro navegador.

El 21 de octubre de 2016 se produjo un gran ataque DDos, con origen en Estados Unidos y que afectó también a Europa. El objetivo de este ataque fue Dym, uno de los proveedores de DNS más importantes, pero resultaron afectados diversos servicios desde las redes sociales, como Twitter, a sistemas de pago, como PayPal.

Blockstack permite acceder a una navegación más segura donde los datos están descentralizados y no almacenados y controlados por unas pocas empresas. Mediante este navegador los usuarios somos los dueños de los datos.

4.1.3. Almacenamiento

Es un hecho que los datos de navegación se almacenan en unos pocos centros de datos, susceptibles a ataques, como el señalado en el apartado anterior, a robo de los mismos o a comercialización por parte de las empresas, como quedó de manifiesto tras el escándalo de Cambridge Anaytica.

Entre otras, las plataformas **Storj** y **Sia** utilizan la tecnología Blockchain para almacenar en la nube los datos, sin riesgo a que sean explotados por piratas informáticos y sin ningún tipo de censura, ya que están descentralizados. Los datos los almacenan los propios usuarios que prestan espacio de almacenamiento en su propio PC, aunque no pueden acceder a ellos ya que no son suyos.

4.1.4. Donaciones

Según la Fundación Lealtad, cuya misión es fomentar la confianza de la sociedad en las ONG para lograr un incremento de las donaciones, así como de cualquier otro tipo de colaboración, para que una donación sea eficaz es necesario conocer cómo se van a gestionar los fondos recaudados. Para ello, el donante tendría que hacer un seguimiento a través de la información publicada en por la ONG. Aquí se encuentra el principal problema: ¿cómo sabemos que esa información es real y fidedigna y que los datos no han sido falseados?

Alice y **Bitgive** son dos plataformas de financiación social basadas en Blockchain que permiten al donante rastrear el destino final sus donaciones. Su funcionamiento es simple: conectan a los donantes con las ONG's y a tiempo real los primeros pueden conocer en qué se va gastando su donación. No habrá que esperar al informe anual, donde los datos podrían ser susceptibles de falseo, y se sabría qué cantidad real se destina a la ayuda humanitaria.

4.1.5. Registros médicos

En la actualidad, hay más de 236 millones de inmigrantes en el mundo de manera legal, y se calcula que esta cantidad se triplica si se tiene en cuenta la inmigración ilegal y la motivada por conflictos en el país de origen. Uno de los problemas de la inmigración es que muchos datos del individuo se pierden, como pueden ser los títulos académicos o los registros médicos.

Afia y **Akiri** permiten almacenar los datos de salud en la nube. Los usuarios pueden administrar sus registros médicos y dar acceso a ellos a los proveedores de atención médica que desee; de igual forma puede cancelar ese acceso a tus datos. Mediante estas plataformas los individuos tendrían recopilados sus datos médicos y fácil acceso a los mismos.

4.1.6. Registros académicos

En el ámbito educativo, las ventajas que ofrece la Blockchain son enormes. El uso de esta tecnología permitiría a los estudiantes acceder a sus datos académicos sin necesidad de consultarlos en las distintas instituciones donde haya cursado estudios. Además, se haría imposible falsear los datos académicos de los expedientes modificándolos a posteriori.

La Universidad de Oxford ha desarrollado **Woolf**, la primera Universidad Blockchain del mundo. Mediante **Woolf**, Oxford se ha convertido en el primer centro académico del mundo que emplea tecnología Blockchain para registrar los movimientos de sus ordenadores. Gracias a ello, nadie pueda eliminar o modificar lo que ya se haya anotado.

4.1.7. Comercio on-line

Los pequeños comercios muchas veces deben utilizar plataformas como Amazon o EBay para poder distribuir sus productos, lo cual merma sus ingresos por una doble vía: la cuota que deben abonar a las compañías y la reducción del precio de sus productos, ya que en primera instancia el comprador opta por el producto de menor coste.

La plataforma **OpenBazaar** ofrece al empresario configurar sus propias tiendas de comercio electrónico al margen de las grandes plataformas de venta. Uno de los problemas que presenta es que el pago debe realizarse en bitcoins, lo cual restringe el acceso a potenciales compradores, si tenemos en cuenta que el cambio oficial era de 1 bitcoin = 10.000 $ en febrero de 2018.

4.1.8. Informática colaborativa

Mediante la plataforma **Golem** los usuarios pueden vender potencia de computación que sus ordenadores no utilizan para, entre otros usos, crear gráficos de alto calibre o realizar tareas criptográficas. Se trata por tanto de una red de alquiler de energía de CPU basada en Ethereum para liquidar pagos entre proveedores, solicitantes y desarrolladores de software.

4.2. Smart Contract

Un contrato inteligente, también conocido por su término anglosajón Smart Contract, es un código o protocolo informático que permite por una parte verificar a los firmantes del contrato y, por otra, hacer cumplir el mismo de manera automática, agilizando de manera clara los trámites de los sectores implicados.

Este término fue acuñado en 1997 por el jurista y criptógrafo Nick Szabo. Pese a definir el concepto teóricamente, era imposible hacerlo realidad con la infraestructura tecnológica existente. Sin embargo, la tecnología Blockchain y los bitcoins permiten que ya se puedan llevar a la práctica.

En la actualidad los contratos requieren de forma escrita y en algunos casos, como el contrato de compraventa de una vivienda, de la necesaria intervención notarial, lo cual acarrea un mayor coste de la transacción. Además, ciertas cláusulas de los contratos pueden estar sujetos a la interpretación que cada una de las partes le den, lo que en caso de conflicto requiere la intervención de un tercero.

Mediante un Smart Contract se elimina esta problemática de la interpretación, ya que, al basarse en un código escrito en lenguaje de programación, los términos del contrato no son más que puras sentencias y comandos en el código que lo forma.

Para sintetizar, hay tres ventajas principales asociadas al uso de estos contratos inteligentes:

- ✓ Transparencia: en todo momento conoceremos el punto de ejecución en que se encuentras el contrato. Por ejemplo, en el caso de un vehículo en un taller, el estado de la reparación.
- ✓ Seguridad: los datos y la información están seguros y no son susceptibles de falsificación.
- ✓ Gestión: se optimizan los recursos con la intervención de la tecnología.

Sin embargo, también presentan una serie de desventajas que dificultan su uso y extensión a mayor número de personas:

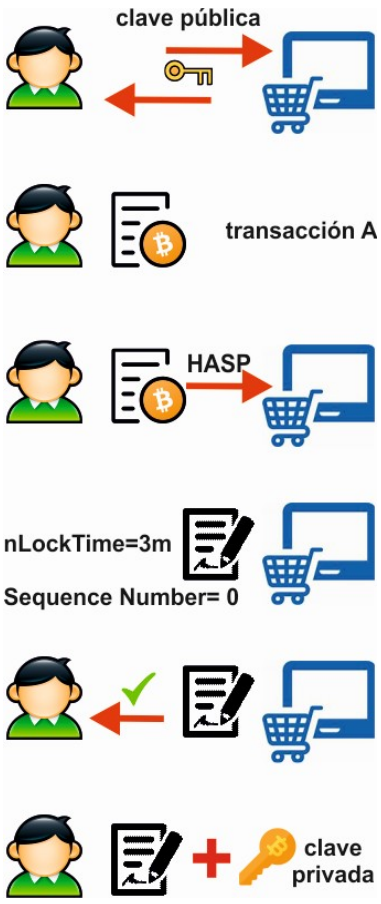
- ✓ El contrato no es modificable y no tiene en cuenta situación surgidas con posterioridad a la firma del mismo.
- ✓ Se precisa contar con formación informática para poder programarlos.
- ✓ Hay que disponer de conocimientos legales para conocer la regulación y legislación de cada territorio, que afectarán a la validez del contrato.

4.2.1. Funcionamiento

El código del Smart Contract que contiene las normas y acuerdos del contrato, se almacenaría en la Blockchain.

Este contrato por estar en Blockchain en inmutable de forma que no se pueden modificar sus reglas, y descentralizado por lo que se cumplen los acuerdos financieros sin depender de sistemas judiciales. Además, un Smart Contract se puede formar sin conocerse, a pesar de ser tratarse de un proceso completamente seguro.

A continuación, se muestra un ejemplo de creación de un Smart Contract durante la compra online financiada en 3 meses:



1. **Usuario y web comercial se envían sus claves públicas.**
2. **Usuario crea (sin transmitir a la web) una transacción con los datos de compra.**
3. **Usuario envía a la web el HASP de la transacción creada.**
4. **La web crea la transacción "contrato" con el código de normas y acuerdos. Ej: "nLockTime" indica que la transacción no se podrá añadir a bloque en 3 meses (reserva fondos).**
5. **Web envía transacción "contrato" al usuario para que lo verifique. "Sequence Number"=0 indica que el contrato podrá ser modificado.**
6. **El usuario firma el contrato con su clave privada, y tras 3 meses se ejecutará el contrato**

Figura 10: Funcionamiento Smart Contracts

Aun así, en ocasiones va a resultar imprescindible acudir a agentes externos, denominados oráculos, que verifiquen el cumplimiento de una condición. Estos oráculos son instrumentos informáticos que validarán las condiciones previstas en los Smart Contracts, utilizando información externa para decidir si una cláusula del contrato ha sucedido o no. Una vez obtenida la información, el contrato se ejecutaría.

4.2.2. Aplicaciones

- Ejecución inmediata

  Una de las aplicaciones inmediatas y que más agradarán a las partes del Smart Contract, es que podrá hacer cumplir los términos del mismo sin necesidad de acudir a los sistemas arbitrales y judiciales, evitando así demoras y costes.

- Sector seguros

  En el sector de seguros, se presentan dos ventajas importantes. Por un lado, se eliminarían los trámites burocráticos que a veces se presentan cuando se plantea una reclamación ante la compañía de seguros. Por otro lado, se agilizaría el proceso de pago ante un siniestro: detectado el mismo y sin necesidad de dar parte al seguro, se realizaría de manera automática.

- Compraventa de mercancías

  En el caso de los contratos de compraventa de mercancías, el comprador del bien o servicio abonaría el pago a la cuenta del contrato y el mismo Smart Contract supervisaría a través del programa de mensajería de la empresa que va a efectuar la entrega que la mercancía se ha transferido al comprador. Una vez realizada la misma, el Smart Contract realizaría el ingreso de la cantidad al vendedor.

- Fallecimiento

  Una de las preguntas claves cuando una persona fallece es si ha hecho o no testamento, para lo cual hay que solicitar el certificado de actos de última voluntad. Mediante un proceso automatizado, basado en Smart Contract, se verificaría la inscripción del fallecimiento en el Registro Civil y se procedería a la ejecución de la herencia, sin necesidad de recurrir a la figura del albacea.

- Control del gasto

  Ya se trate de fondos públicos o privados, el Smart Contract permitiría limitar el gasto de un proyecto ya sea temporal o geográficamente. Estamos ante lo que se denomina dinero programable útil que facilita el control de los presupuestos y evitaría, en el ámbito público, la corrupción y la utilización fraudulenta de los contratos públicos y las subvenciones: se realizaría una fiscalización del gasto a tiempo real sin esperar a los mecanismos de control establecidos.

4.3. Futuros aplicativos de Blockchain

Además de los usos actuales de la Blockchain, hay otros usos que podrían darse de este sistema en el futuro y que garantizarían una mayor seguridad de los datos y una mejor eficiencia y eficacia de los procesos.

- Entidades Gubernamentales

  En la actualidad, muchos de los procedimientos realizados por las entidades públicas tienen demora debido a la petición de información a otras entidades. La Blockchain permitiría que se accediera a esta información en tiempo real y se recortara los tiempos de espera. Pero no sólo esto, sino que se tendría mejor y mayor control sobre las actividades de los cargos electos, lo que ayudaría a reducir la corrupción y aumentar la transparencia.

- En la Industria 4.0

  Por Industria 4.0 se entiende una nueva forma de organizar los medios de producción con el que fuera posible una mejor adaptación a las necesidades y una asignación más eficiente de los recursos. Para llegar a esta modelo industrial es necesario que las empresas confíen en que datos sensibles, como pueden ser los modelos de producción o las patentes, sean gestionados con fiabilidad y seguridad.

  El uso de la Blockchain permitiría que las empresas fueran capaces de acceder a los datos en un entorno estable y seguro.

- Logística

En el análisis del sector postal y del sector de la mensajería y la paquetería de la Comisión Nacional de los Mercados y de la Competencia del año 2017, se señala los envíos de paquetería han aumentado un 56,3% desde el año 2013. Es evidente que los envíos van a generar una gran oportunidad de negocio durante la próxima década.

Hay dos proyectos pioneros en marcha que convienen destacar: por un lado, un grupo de empresas capitaneados por Bosch y Cisco pretender llevar la tecnología Blockchain a los dispositivos conectados que se empleen en la logística o la energía; por otro, un grupo de empresas norteamericanas, entre las que destacan Nestlé o Unilever, pretenden que la Blockchain monitorice la cadena de suministro de alimentos y así mejorar la seguridad de estos productos de consumo.

- Votaciones

En la actualidad en nuestro país sólo es posible votar de manera presencial para así asegurar la identidad del votante y que no se haya suplantado la misma. El uso de la Blockchain garantizaría un nivel de seguridad tal que fuera imposible suplantar la identidad del votante, así como otorgar de una mayor comodidad al mismo ya que no sería necesario que se desplazara a la oficina electoral o utilizara el servicio de voto por Correos: se podría votar desde el propio móvil.

La empresa española “Agora Voting”, actualmente desaparecida, desarrolló su propio sistema electoral utilizando seguridad basada en métodos criptográficos. Sin embargo, para alcanzar este objetivo es necesario la modificación de la legislación vigente, que en el caso español pasa por modificar la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral y en la actualidad la única iniciativa parlamentaria en relación con el voto electrónico limita su uso a los españoles residentes en el extranjero.

5. Otras criptodivisas

5.1. Panorama actual

Bitcoin, Etherum, Ripple, Bitcooin Cash, EOS, Litecoin, Cardano, Stellar, IOTA, TRON, WLADIHUM, … Son cada vez más los tipos de criptomonedas y cada vez son más codiciadas por los especuladores.

La naturaleza de este nuevo sistema de moneda se ampara en su descentralización, privacidad, agilidad, ausencia de intermediarios para tener buena acogida en los usuarios, y poco a poco a los mercados e inversores

A continuación, se muestran las cuatro principales criptomonedas actuales (sin contar con la primera, Bitcoin) que circulan por el mercado:

5.1.1. Etherum (ETH)

Es una plataforma de código abierto creada en Julio de 2015 por Gavin Wood, Jeffrey Wicke y heikoheiko. Está basada en Blockchain y enfocada a los contratos inteligentes. Su criptomoneda llamada “Ether” es intercambiable entere cuentas de Etherum, y se utiliza para compensar a los nodos mineros igual que pasaba en Bitcoin.

Etherum fusiona descentralizadamente mediante máquinas virtuales a modo de nodos llamados Etherum Virtual Machine (EMV). Los contratos formados en Etherum son tan diversos como intercambios financieros, sistemas de votación propiedad intelectual u organizaciones descentralizadas autónomas.

5.1.2. Bitcoin cash

Bitcoin en efectivo se trata de una rama de Birtcoin creada el 1 de agosto de 2017 por desarrolladores de la comunidad de Bitcoin con objeto de aumentar la velocidad en las transacciones a 8 MB. Ese día se separó la cadena de bloques actual de Bitcoin en dos cadenas válidas: Bitcoin original y la nueva Bitcoin cash cuya moneda es el BCH.

5.1.3. Ripple

Ripple más que una criptomoneda se trata de una red de transacciones descentralizada extremo a extremo, más que de una criptomoneda. Se considera un sistema más seguro que Bitcoin, y está enfocado en la liquidación bruta en tiempo real de forma rápida y barata, por lo que la red Riple ya está instaurada en bancos. A pesar de que su divisa en el Ripple, la red admite todo tipo de monedas fiduciaria.

Como sistema de pago podría interconectar sistemas de pagos tradicionales y alternativos con la ventaja de plataformas como PayPal pero sin un ente centralizado.

5.1.4. Littecoin

Basado técnicamente en Bitcoin, fue creado como alternativa a Bitcoin con los objetivos de reducir el procesamiento de bloque de 10 a 2,5 minutos, producir cuatro veces más de moneda que Bitcoin, y utilizar un script de prueba de trabajo que ayude a los mineros, evitando el esfuerzo computacional y el gasto de energía.

5.1.5. Cuadro comparativo

A continuación, se muestran los aspectos más significativos de las 5 principales criptomonedas del mercado:

Tabla 1: Comparativa de las principales criptomonedas

	Bitcoin	**Etherum**	**Bitcoin Cash**	**Ripple**	**Litecoin**
Lanzamiento	2009	2015	2017	2012	2012
Creador	Satoshi Nakamoto	G. Wood, J. Wilcke,	Comunidades Bitcoin	Chris Larsen	Charlie Lee
Tecnología	BlockChain	BlockChain	BlockChain	BlockChain	Blockchain
Algoritmo	SHA-256	Ethash	SHA-256	ECDSA	Scrypt
Velocidad transacción	Lenta	Lenta	Rápida	Muy rápida	Rápida
Tipo	Moneda	Moneda	Moneda	Red	Moneda
Precio actual	7.487$	591$	1101$	0,6525$	119$
Capitalización	77.000m	36.000m	10.000m	9.000m	3.000m
Max.cantidad	21m	100m	21m	100 mil m	84m
Precio actual	7.487$	591$	1101$	0,6525$	119$

5.2. Regularización

El dinero en forma criptográfica ha sufrido un espectacular auge en el último año, superando los 300 mil millones de dólares desde abril de 2017. Este rápido ascenso requiere comprender los peligros en lo referente a la seguridad, y controlar las criptodivisas establecidas, así como las que surjan.

Para crear una criptomoneda, primero es necesario diseñarla, después implementarla mediante software, y por último poner éste a disposición de toda la comunidad para que surjan mineros que mantengan la actividad de la criptomoneda creada.

Todo este desarrollo requiere de una financiación, y la principal forma de realizarlo es mediante una ICO (Oferta Iniciales de Moneda - Initial Coin Offerings-). Los desarrolladores de la criptomoneda crearan su moneda virtual mediante un pre-minado, e intercambiaran la criptomoneda obtenida por otras criptomonedas como BitCoin o Etherum (que son intercambiables por dinero real); por ello el proceso de ICO es ofrecer a inversores una nueva moneda a cambio de dinero.

En este aspecto haya que señalar que cualquier proyecto de Blockchain puede basarse en ICO, ya que el Blockchain desarrollado se sostendría sobre unos “tokens” que hacen las funciones de criptomonedas y que se intercambiarían con el inversor.

El objetivo pues de una ICO es recaudar dinero, y el objetico de sus participantes es lucrarse; si bien como cualquier inversión conlleva un riesgo. Un caso de éxito basada en ICO es la criptomenda Etherrum, que antes de lanzarse a la comunidad, recaudó 10 millones de dólares.

Sin embargo, las ICOs tienen problemas intrínsecos a su naturaleza, como la falta de seguridad en el diseño de desarrollo. El ejemplo más actual fue el robo de 50 millones de dólares en Etherum en Julio de 2017 a la ICO formada por once mil personas que invertían en un programa de ordenador (caso “The Dao”).

Por otro lado, las operaciones no están reguladas, por lo que el Gobierno pierde el control del dinero y sus impuestos, y las ICOs podrían utilizarse para actividades delictivas como financiación del terrorismo, por ejemplo.

Ante esta problemática países como China o Corea del Sur ya ha declarado las ICO ilegales, mientras que otros países como Estados Unidos pretende regular la actividad de ICOs y criptomonedeas en 2018, desde la SEC (Comisión de Intercambio y Seguridad -Securities and Exchange Commission-) enfocándose en tres acciones principales:

- Reducir la volatilidad en los criptomercados

  Utilizando informes de requisitos y auditorías mediante herramientas de cumplimiento regulatorio como recientemente realizó la empresa Gecko Governance en aplicaciones de Blockchain. Así se proporcionarán liquidez a los mercados de criptomendas donde los grandes inversores aún son reticentes a la hora de actuar, y se evitaría que entidades individuales manipulen los precios al haber una criptomoneda institucional.

- Reducir las transacciones opacas al gobierno y al escudriño público

  Utilizado un sistema de grabación de transacciones. Si bien esta medida aumentaría los costos de intercambios, y serían los empresarios los que valorarían aceptar los riesgos de una criptomoneda tradicional, o asumir recursos para el control de una de criptomoneda institucional.

- Hacer de las ICOs una opción de inversión viable

  Mediante la obligada presentación de informes de requisitos y libros de contabilidad sobre el proyecto a invertir, herramientas que actualmente no existen y por la que hasta un 80% de las actuales ICOs son estafas

5.3. Futuro en los mercados financieros

El mercado de las criptodivisas se redujo a la mitad desde principios del año 2018, cuando había más de 800.000 millones de dólares en curso hasta la actualidad cuando hay 300 millones de dólares.

sin embargo, son varios los economistas que preveen un gran resurgimiento gracias a Instituciones occidentales que invertirán dando apoyo a los precios, y a los especuladores que contemplan la volatilidad de la criptomoneda como una gran oportunidad.

Así, es muy posible que fondos de inversión y gestores activos participen má activamente en el universo de la ciptomoneda.

Además, la inminente regularización de la actividad por parte de los gobiernos puede acercar más los grandes inversores, creando más demanda, lo que abrirá un amplio campo para nuevos Alcoins (criptomonedas derivadas del código fuente de Bitcoin)

6. Conclusiones

La implantación de la criptodivisas BitCoins, sus derivadas Altcoins, y la potente tecnología Blockchain es un hecho a día de hoy.

Si bien los gobiernos y entidades bancarias siguen siendo reticentes a reconocer esta criptodivisa, son muchas las empresas que implantan este sistema de transacción financiera en sus servicios, y el número de transacciones con BitCoin aumenta de forma exponencial.

La variación de precio del BitCoin es también algo sintomático, valiendo de 0 a 1.000$ desde su origen en 2009 hasta finales del año 2016, y multiplicando su valor hasta nuestros días, cuando su valor supera los 7.000$. Ésta fluctuación junto con la creación constante de otras criptodivisas motiva desconfianza y un futuro incierto a las criptodivisas.

Sin embargo, el protocolo Blockchain sobre el que se basa Bitcoin, dispone de un enorme potencial por su arquitectura segura, transparente y fiable, que ha motivado su implantación en diferentes aplicativos -incluso de organismos gubernamentales-, y que se está desarrollando constantemente en todos los ámbitos empresariales para diversos proyectos.

7. Bibliografía

- Como funiona Bitcoin. Bitcoin Project 2009-2018
  https://bitcoin.org/es/ Consulta: Abril y Mao de 2018

- SANTIAGO MARQUEZ SOLIS.1 mar 2016.
  Bitcoin. Guia Completa de la Moneda del futuro. Barcelona: EDIPE

- Criptomonedas. Información en tiempo real. 2108
  https://es.investing.com/crypto/. Consulta Junio 2018

- Explorador de bloques de Bitcoin
  https://blockchain.info/es. Consulta Marzo 2018

- Consenso. Libro de blockchain
  http://libroblockchain.com/consenso/. Consulta Abtil 2018

- Minar bitcoins.
  https://blog.bit2me.com/es/que-es-minar-bitcoins/. Consulta abril 2018

- Cinco usos del blockchain más allá del bitcoin

  http://www.ticbeat.com/innovacion/cinco-usos-del-blockchain-mas-alla-del-bitcoin/. Conaulta Abrtil 2019