GRADO EN ECONOMÍA

CURSO ACADÉMICO 2021-2022

TRABAJO FIN DE GRADO

Criptomonedas: Medio de pago, tecnología y financiación.

Cryptocurrency: Payment method, technology and financing.

AUTOR: ADRIÁN ARGUMOSA BORBOLLA

DIRECTOR: ADOLFO MAZA FERNÁNDEZ

27 DE SEPTIEMBRE DE 2021

A Rosa Eva

ÍNDICE

RESUMEN

El dinero lleva siendo un método de cambio desde la antigüedad, que con el paso del tiempo y los avances tecnológicos ha ido transformándose. La irrupción de unas nuevas monedas virtuales que buscan características diferentes a las presentes hasta el momento, pretende cambiar la forma de hacer intercambios entre personas. El nacimiento así de la primera criptomoneda, el Bitcoin, creada por Satoshi Nakamoto junto con el Blockchain, la tecnología que lo sustenta y que cambiará la forma de entender el mundo como ya lo hizo en su día Internet, hace preguntarse si puede darse un cambio en la forma de realizar los pagos entre individuos. Para ello es fundamental conocer bien lo que son las criptomonedas, sus características, la volatilidad que presentan, su seguridad, la tecnología en la que se apoyan, la legislación que siguen, como la postura de los países con respecto a ellas. Conocer que existen diferentes proyectos dentro de estas, en el que cada uno va a ofrecer unas cualidades distintas a otras, por lo que se halla una amplia variedad para seleccionar. Por último estas monedas han permitido la aparición de nuevas formas de financiación a las empresas, a pesar de ser inversiones muy arriesgadas, se pueden sacar unas rentabilidades muy notorias.

Veremos lo que pasa en los años futuros. ¿Las criptomonedas han llegado para quedarse o son meramente una burbuja especulativa?

ABSTRACT

Money has been a method of exchange since antiquity times, which with the pass of time and the technological advances has been transforming. The emergence of new virtual currencies that search different characteristics to those present so far, aims to change the way of making exchanges between people. The source of the first cryptocurrency, Bitcoin, created by Satoshi Nakamoto together with Blockchain, the technology that supports it and that will change the way of understanding the world as the Internet already did, makes one wonder if there can be a change in the way of making payments between individuals. For this, it is essential to know well what cryptocurrencies are, their characteristics, the volatility they present, their security, the technology, the legislation they follow, and the position of countries with respect to them. Know that there are different projects within these, in which each one will offer different qualities to others, so there is a wide variety to select from. Finally, these currencies have allowed the emergence of new forms of financing for companies, despite being very risky investments, a notable returns can be obtained.

We will see what happens in the future. Are cryptocurrencies here to stay or are they a speculative bubble?

PALABRAS CLAVE

Criptomonedas, Bitcoin, dinero, Blockchain, transacciones.

ABREVIATURAS

PoW Proof of Work

PoS Proof of Stake

ICO Initial Coin Offering

STO Security Coin Offering

IEO Initial Exchanges Offering

NFT Non-Fungible Tokens

IVA Impuesto sobre el Valor Añadido

ITPAJD Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados

IRPF Impuesto sobre la Renta de las Personas Físicas

IP Impuesto sobre el Patrimonio

FIFO First In First Out

IAE Impuesto sobre Actividades Económicas

P2P Peer-to-Peer

ID Identity Document

DAO Decentralized Autonomous Corporation

SWIFT Society for Worldwide Interbank Financial Telecommunication

DLT Distributed Ledger Technology

RPCA Robust Principal Component Analysis

ASIC Application-Specific Integrated Circuit

DAG Directed Acyclic Graph

OPV Oferta Pública de Venta

MVP Minimum Viable Product

KYC/AML Know Your Customer / Anti-Money Laudering

INTRODUCCIÓN

"Cryptocurrencies are everything you do not understand about money combined with everything you do not understand about computers. " (John Oliver, Last Week Tonight).

Los historiadores datan el origen del dinero en el siglo VII antes de Cristo, en la zona de Turquía, antiguamente conocida como el Reino de Lidia. La importancia de este es sumamente conocida por todos, y es el principal eje por el que se mueve el mundo. Para que sea considerado como un mecanismo de comercialización dota de mecanismos de legalidad y de confianza para ser usado como medio de pago por los agentes económicos en sus trueques, desempeñando funcionalidades como depósito de valor y unidad de cuenta. Con el paso de los años el dinero y los métodos de pago han ido evolucionando constantemente, desde el pago con metales, al pago a través del propio teléfono móvil y es que tras la llegada de internet se ha abierto un abanico de posibilidades. Los incesables avances de la tecnología en las últimas décadas han afectado a todo tipo de sectores incluido el económico.

Aplicando la tecnología a los métodos de pago, ya desde antes del año 2000, varios especialistas en criptografía buscaban una manera para realizar transacciones monetarias de forma anónima mediante la criptografía, el primero fue David Chaum con “eCash” y “Digicash”, aunque en estas plataformas la emisión y el pago eran centralizados. Pero es el científico y cypherpunk Wei Dai es quien introduce por primera vez la idea de criptomoneda. Desarrollo el B-Money, un medio con el que se buscaba libertad ante gobiernos y autoridades centrales, descentralizando las transacciones, pero este no llego a ponerse en marcha, aunque, es un precedente muy importante para que en el año 2009 surja la primera criptomoneda, bajo el alias de su desarrollador “Satoshi Nakamoto”, del que se desconoce su identidad o identidades. A partir de este momento nace un creciente interés por todo el ecosistema de las criptomonedas y la forma en la que pueden cambiar el mundo.

El objetivo que se busca en este trabajo es presentar el entorno de las criptomonedas, debido al importante auge que están cobrando en los últimos años y el cual es motivo de interés para muchos. Se planteara la exposición de estas para entender cómo funcionan este tipo de divisas y así poder plantearse si estas pueden ser consideradas como un medio de pago que pueda establecerse en el mundo en los años próximos. Con ello se dividirá el trabajo en cuatro partes, siendo la primera una presentación de las criptomonedas donde se abordaran los orígenes del dinero digital como tal, además de hablar de sus características, la comercialización, los tipos de tokens y la legislación que puede existir dependiendo de la actividad. La segunda parte se centra en toda la tecnología que está detrás de ellas y en explicar cómo se mueven las transacciones por la cadena de bloques. La tercera parte se presentan los proyectos de criptomonedas más importantes del ecosistema en donde se pretende mostrar la variedad de propósitos que existen en las diferentes empresas creadoras. Por último, en el capítulo final, se focaliza la atención en las nuevas formas de financiación para “starts-up” a través de las criptomonedas.

CAPÍTULO 1. ORIGEN, CUALIDADES Y COMERCIALIZACIÓN.

1.1. INICIOS

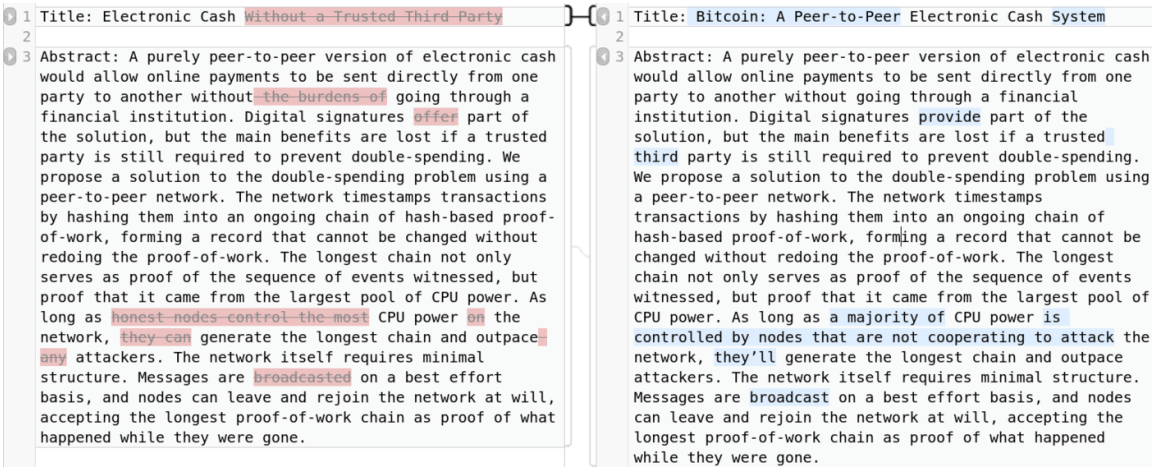
Como se ha comentado en la introducción, varios especialistas en criptografía buscaban un medio con el que poder realizar transacciones fiduciarias sin la supervisión de gobiernos y organismos institucionales. David Chaun es reconocido por ser el inventor del dinero digital, además de ser uno de los referentes del movimiento Cypherpunk de finales de los 80. Fue el organizador de las primeras conferencias sobre criptografía que se dieron lugar en Santa Bárbara (California), desde el 1982 (CRYPTO ´82), donde puso la primera piedra en el camino proponiendo un protocolo de dinero digital que sería verdaderamente anónimo, en el que los pagos digitales se realizarían utilizando una "firma ciega".

Tras todas sus investigaciones, David llega a crear DigiCash Inc., en 1990, una empresa de servicios de dinero electrónico. Con ella despliega eCash, concebido como dinero criptográfico anónimo, en el que se utilizó el sistema de micro pagos a través del banco Mark Twain de EE.UU.

Posteriormente otro criptógrafo de la comunidad Cypherpunk, el informático chino Wei Dai licenciado en la Universidad de Washington, ideo el llamado "B-Money", medio con el cual se podían hacer más eficientes las transacciones, siendo un tipo de sistema de seguro, electrónico, distribuido y anónimo, el sistema se regiría de manera similar al que se rige Bitcoin. Dai propuso dos formas para formular el sistema, la primera se basa en el uso de una Prueba de Trabajo (PoW) para crear el dinero y utilizar Hashcash para realizar la minería. La segunda planteaba el uso de un subconjunto de servidores, que se encargan de organizar las transacciones, este sistema es similar al esquema de Prueba de Participación (PoS), que sin embargo nunca llego a ejecutarse.

Una comunidad es definida por el nivel de cooperación de sus participantes y una cooperación eficiente requiere un medio de intercambio (dinero) y una forma de enforzar los contratos. Tradicionalmente estos servicios han sido provistos por el gobierno o por instituciones financiadas por el gobierno, y solo por entidades legales. (Wei Dai ,1998).

Bajo la base teórica que dejo planteada Wei Dai, en el año 2009 surge definitivamente la primera criptomoneda como tal, el Bitcoin. Su creador o grupo de creadores bajo el alias Satoshi Nakamoto, diseño un sistema más eficiente para la aprobación de la red. El sistema propuesto por Dai fue incluido en el "Libro Blanco del Bitcoin" debido a sus múltiples similitudes. Nakamoto envió meses antes el borrador del libro a Wei en el que aun ni siquiera se llamaba Bitcoin, sino, "Dinero electrónico sin un tercero de confianza".



Title: Electronic Cash ~~Without a Trusted Third Party~~

Abstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without ~~the burdens of~~ going through a financial institution. Digital signatures ~~offer~~ part of the solution, but the main benefits are lost if a trusted 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 ~~honest nodes control the most~~ CPU power ~~on~~ the network, ~~they can~~ generate the longest chain and outpace ~~any~~ attackers. The network itself requires minimal structure. Messages are ~~broadcasted~~ 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.

Title: Bitcoin: A Peer-to-Peer Electronic Cash System

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.

Figura 1. Documento enviado por Nakamoto a Dai donde aún no contenía el nombre Bitcoin (izquierda). Fuente: gwern.net.

La inspiración de la creación del Bitcoin fue sustituir a largo plazo el dinero físico como tal, ya que esta surge a partir de la crisis financiera de 2008 y la disminución del dinero en circulación. Nakamoto quiere transmitir una nueva idea de entender el método de cambio en las transacciones, esto lo plasma en el libro que generaliza, "Bitcoin: un sistema de dinero en efectivo peer-to-peer", en el que enseña la tecnología en la que se basaba la moneda para efectuar las transacciones.

La primera transacción con bitcoins tuvo lugar en 2010, Laszlo Hanyecz programador de la web "BitcoinTalk" publico en un foro el 18 de Mayo que pagaría 10.000 bitcoins a cualquier persona que le llevara a casa 2 pizzas. El valor del Bitcoin en ese momento era de unos 0.004$ cada uno. El mensaje fue el siguiente:

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in 8oe at8e for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something 8oe at and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc… just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

Fuente: https://bitcointalk.org/index.php?topic=137.0

1.2. CARACTERÍSTICAS

Generalmente las criptomonedas siguen un mismo tipo de características que las hace únicas:

- **Virtualidad:** Están exentas de apariencia física, son únicamente digitales.
- **Descentralización:** La regulación de los movimientos de las transacciones ejecutadas por los distintos individuos no están controlados por ningún tipo de institución.
- **Privacidad**: A pesar de que al realizar operaciones, necesitamos registrarnos en un Exchange (monedero virtual), por seguridad, con nuestros datos personales, las transacciones que se realicen serán de manera anónima ya que se utiliza una dirección de criptografía (alfanumérica).
- **Transparencia:** Todas las transacciones de las criptodivisas validadas por los mineros, quedan guardadas en la cadena de bloques.
- **Volatilidad:** Una característica específica de este mercado con respecto a otros como pueden ser el mercado de acciones es la volatilidad. Es difícil predecir el signo que va a tomar una criptodivisa, haciendo que el riesgo y la rentabilidad sea de una cota mayor. Esto es debido a la escasez del mercado, ya que hay un gran poder de mercado de ciertos usuarios.
- **Coste y rapidez:** Las tarifas de transacción no son costosas, puedes enviar criptomonedas a cualquier parte del mundo con una mínima comisión, debido a que no hay intermediarios (peer-to-peer), esta comisión solo se cobra por el proceso de comprobación y envió de la operación, además las transacciones son enviadas en unos pocos segundos, una vez recibida, la verificación de los mineros suele tardar alrededor de 10 minutos, aunque puede ser en un menor tiempo, dependiendo de la criptomoneda.
- **Seguridad:** Se utiliza la criptografía para la seguridad a la hora de realizar cobros y pagos, haciendo así que no pueda darse la posibilidad de falsificaciones.
- **Internacionalidad:** Representan la economía del grupo de personas que las usan a nivel mundial, donde se puede comercializar con ellas en diferentes países del mundo.

Figura 2. Fuente: EAE Bussiness School.

1.3. EXCHANGE

Espacio donde se dinamiza la compra/venta de criptomonedas, hay que distinguir a estos de los monederos (exclusivamente para recibir/guardar/enviar criptos) y de las casas de cambio (donde se convierte el dinero FIAT en criptomonedas y viceversa).

Hay algunos exchanges que no aceptan el dinero FIAT, por lo que para empezar a operar en estos hace falta comprar las criptomonedas en una casa de cambio, aunque cada vez más aceptan las monedas tradicionales para operar como; Kraken, Binance, FTX, Bitfinex…

Es interesante manejar varios exchanges a la hora de operar, para diversificar riesgo, poder operar con diversas criptomonedas (no todos los exchanges pueden tener las mismas), distintos tipos de precios al momento, problemas con la liquidez, operaciones de arbitraje…

1.4. TOKENS

Término utilizado en la economía digital, estos son activos digitales, es decir, unidades de valor que son creadas por una entidad privada donde posee un valor aceptado dentro comunidad y que se basa en la tecnología Blockchain.

El significado de token es más genérico que el de criptomoneda, ya que se puede aplicar a más ámbitos que el únicamente monetario, el objetivo de los tokens es la representación de cualquier cosa, desde casas a objetos de colección, aunque pueden utilizarse como medio de pago, se enfocan en la representación de valor.

Existen varios tipos de tokens:

Utility Token: Estos ofrecen el acceso a servicios de la empresa que les crea, suelen crearse para conseguir financiación, como veremos más adelante con las ICO.

Security Token: Activo digital que se vincula a valores financieros tradicionales. Se han convertido en una forma segura de inversión y financiación para proyectos con tecnología Blockchain, gracias a que el valor del token deriva de activos regulados.

Equity Token: Se vincula estrechamente con las acciones tradicionales, la posesión de estos representa una proporción de propiedad de un activo o empresa.

NFT: Representan activos digitales únicos y que no pueden ser divisibles en partes. Pueden ser artículos de colección únicos, coleccionismo del mundo real, obras digitales, incluso tweets.

Jack Dorsey, director ejecutivo de Twitter, vendió este año el primer tweet que se publicó en 2006 en la famosa plataforma, con el siguiente mensaje: “just setting up my twttr”.

El primer tuit de la historia, vendido por 2,9 millones de dólares. *La venta, una muestra del auge del coleccionismo digital gracias a los llamados ‘tokens no fungibles’ (El País, 2021)*

Es en este año 2021 donde se ha producido un boom por este tipo de tokens, en donde los creadores de la obra conceden la licencia de explotación a los poseedores del NFT que representa.

1.5. LEGISLACIÓN

Una de las mayores preocupaciones de las personas cuando conocen este ámbito es el correspondiente con la legalidad y la fiscalidad que siguen estas monedas virtuales. Cada país posee una legislación diferente y se enfrenta a un constante cambios en el tiempo. Ante algo tan nuevo como son las criptomonedas todavía no existen leyes específicas que se encarguen de regularlas tanto a ellas como a la tecnología que las respalda, pero cierto es que a día de hoy hay una serie de países que han decidido intervenir o prohibir estas divisas. En países como Bolivia, Marruecos, Argelia y Egipto está prohibido la posesión y negociación con bitcoins y los demás altcoins. En otros países como Canadá, China, Qatar y Nigeria las regulaciones están orientadas a prohibir los préstamos bancarios. En cambio sí que hay países que apuestan por estas, como Venezuela que ha creado su propia criptomoneda conocida como “Petro” o en El Salvador donde han aprobado una ley para que el 7 de septiembre de este año se considere al Bitcoin como moneda de curso legal, algo que ha traído una serie de protestas entre sus habitantes.

La regulación que se sigue en España es la de la doctrina de la sentencia del 22 de octubre de 2015 del Tribunal de Justicia de la UE, en la que se consideró al Bitcoin y al resto de criptomonedas como medios de pago, en vez de como valor financiero, por lo que no está sujeto a IVA ni al ITPAJD.

Hay que tener en cuenta que hay varios tipos de actividades dentro de las criptomonedas por lo que la fiscalidad variará dependiendo cual sea:

Compra y venta: Si el individuo realiza actividades de comprar, vender o convertir las criptomonedas en dinero fiat se deberá declarar estas operaciones dentro del IRPF (siguiendo el método contable FIFO) y en el IP debido a que se produce en todo caso una alteración patrimonial del individuo ya sea en forma de ganancia o pérdida.

Transacciones de bienes y servicios: A la hora de comprar algún tipo de bien o pagar por servicios recibidos con criptomonedas, siempre que la empresa o entidad las admita, las operaciones estarán sujetas al tipo de IVA que corresponda en ese caso.

Minería: Se concibe como una actividad empresarial que sigue como tal obligaciones fiscales; estar dado de alta en el IAE (epígrafe 83: Otros servicios financieros), exponer declaraciones trimestrales, además del IRPF anual que puede ser de dos formas; rendimientos por actividades económicas o ganancias patrimoniales. Si se desea realizar esta actividad es obligatorio darse de alta en la Seguridad Social como autónomo, lo que implicará que pueda reducir gastos con la cuota de autónomos o amortizar el hardware informático junto a toda la instalación y energía que necesite para dicha actividad.

ICO: En las Inital Coin Offering su regulación con la compra de tokens sigue la misma regulación que las criptomonedas. Entre los Utility Token, Security Token y los NFT se valoran como capital mobiliario.

Holdear: Esta actividad que es seguida por muchos “traders”, puede verse regulada si el stock de las criptomonedas se encuentra guardado en algún exchange situado en el extranjero, entonces es de obligado cumplimiento la declaración de las criptomonedas con el modelo 720, en exchanges que superen la cifra de 50.000 euros a fecha de 31 de diciembre.

CAPÍTULO 2. TECNOLOGÍA BLOCKCHAIN.

Para entender cómo se mueven las criptomonedas es fundamental entender el concepto de Blockchain, siendo esta la tecnología que promete cambiar el mundo como ya lo hizo Internet en su momento.

Satoshi introdujo en el Libro Blanco una nueva tecnología revolucionaria con la que iba a funcionar el Bitcoin llamada “Blockchain” o “Cadena de Bloques”, una especie de “libro mayor” de contabilidad P2P en el que quedan registradas todas las transacciones que se realizan entre los usuarios de una forma segura, privada, sin ningún tipo de intermediario y con el funcionamiento a través de tecnología criptográfica.

El sistema de distribución P2P es uno de los más usados en el tráfico de datos en Internet, pero en los intercambios de este tipo en criptomonedas el funcionamiento es distinto. El intercambio P2P relacionado a una plataforma Blockchain habilita la transacción de criptomonedas a partir de un software pre-programado, en el que no es necesario terceras personas, poniendo directamente en contacto a compradores y vendedores.

2.1. FORMACIÓN Y FUNCIONAMIENTO DEL BLOCKHAIN

La Blockchain se estructura en distintos nodos, siendo ordenadores conectados a la red, haciendo que esta sea descentralizada y utilizando el mismo tipo de protocolo. Esto es denominado “consenso” siendo de vital importancia en la Blockchain, ya que este protocolo verifica y ejecuta las transacciones haciendo que sean inalterables.

El proceso por el que pasa una transacción en la Blockchain es el siguiente:

Nos encontramos con dos individuos, A y B, el individuo A desea enviar dinero a B, entonces se crea una transacción hacia el individuo B. Esta transacción que se va a realizar se representa como un “bloque” en la red. Este bloque se emite a todas las partes de la red y tiene que ser validado por los distintos nodos que existen en ella. Una vez que se acepta la transacción se añade el bloque a la Blockchain, como si fuera un apunte a un libro de contabilidad. A continuación la transacción es verificada y se procede a ejecutar el movimiento de dinero hacia el individuo B. Estas transacciones resultan inalterables y son muy seguras para evitar robos, hackeos y estafas.

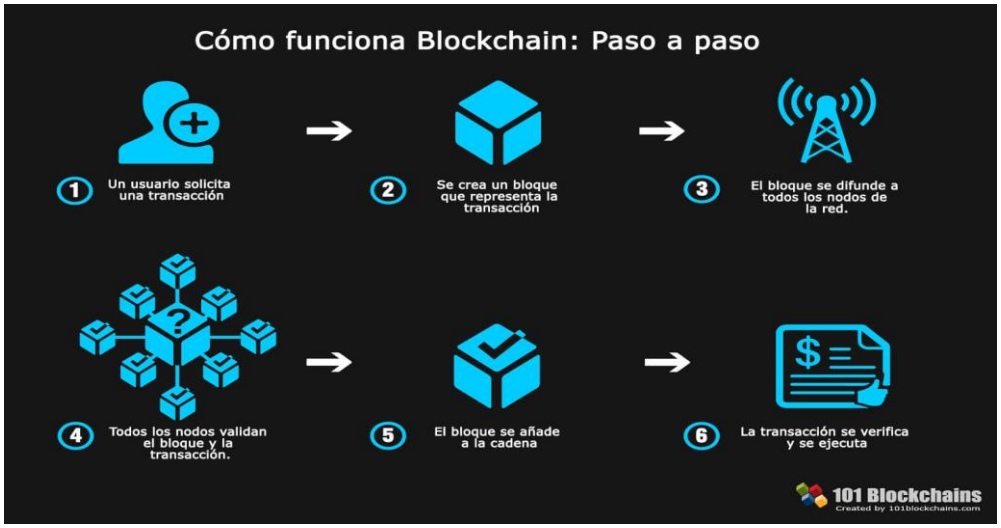


Figura 3. Representación esquemática del proceso de una transacción entre dos individuos. Fuente: 101 Blockchains.

2.2. MINADO

Los dos protocolos de consenso que más se utilizan en la actividad de minado, responsable de validad las transacciones, son la PoW (Proof of Work) y la PoS (Proof of Stake). La principal diferencia entre ambas es que que la PoW necesita recursos externos como hardwares, en cambio en la PoS no son necesarios.

En la **PoW** al realizarse una transacción, son los nodos mineros repartidos por todo el mundo los encargados de la resolución del problema matemático creado con una función "hash" que se emite en la red, suele ser cada 10 minutos que es lo que se tarda aproximadamente en resolverse el acertijo (aunque el tiempo de resolución puede variar dependiendo la criptomoneda). El nodo que resuelva correctamente el problema (con la validación de los demás nodos) se llevará la recompensa más el "fee", esto cuenta como un nuevo bloque que se añade a la cadena.

El problema de este consenso es la necesidad de un potente equipo informático y del gasto energético que supone (electricidad, refrigeración, mantenimiento…), pero cabe la posibilidad de unirse a los llamados "pools mineros", grupos de minado que se forman para tener un mayor poder computacional.

Tras el minado de cierta cantidad de bloques, que varía dependiendo la criptomoneda, se produce una re calculación de la capacidad de cómputo de la red para modificar la complejidad del problema a la actualidad. Esto hace que cada vez sea más complicado minar un bloque y la cantidad percibida sea menor.

En criptomonedas que utilizan este consenso como Bitcoin, cada 210.000 bloques se reduce la recompensa que reciben los mineros a la mitad**,** conocido como "halving" (proceso automático en el que la recompensa por bloque minado de cierta criptomoneda se fracciona a la mitad con el objetivo de disminuir el nivel de emisión), actualmente está recompensa se encuentra en 6,25 BTC por cada bloque minado.

Satoshi Nakamoto forjo en Bitcoin un límite máximo de 21 millones de bitcoins que se van liberando al realizarse las transacciones y los mineros las acepten, una vez alcanzado este límite los mineros solo serán pagados con las comisiones.

Figura 4. Imagen de una granja de minado. Fuente: hardzone.es

La confirmación de transacciones con **PoS** es diferente y este surge como respuesta a los altos costes de energía de la **PoW**, donde además los cálculos criptográficos son más simples. Se fundamenta en un algoritmo de consenso con tecnología Blockchain, en donde la probabilidad de recibir la recompensa por encontrar un nuevo bloque es superior para los que tienen una mayor cantidad de criptomonedas almacenadas durante más tiempo.

Este consenso se fundamenta en que quienes tienen una mayor cantidad de la moneda están más interesados en salvaguardar la integridad y el funcionamiento de la red que otorga el valor a las monedas, por lo que son más apropiados para proteger la red de ataques externos.

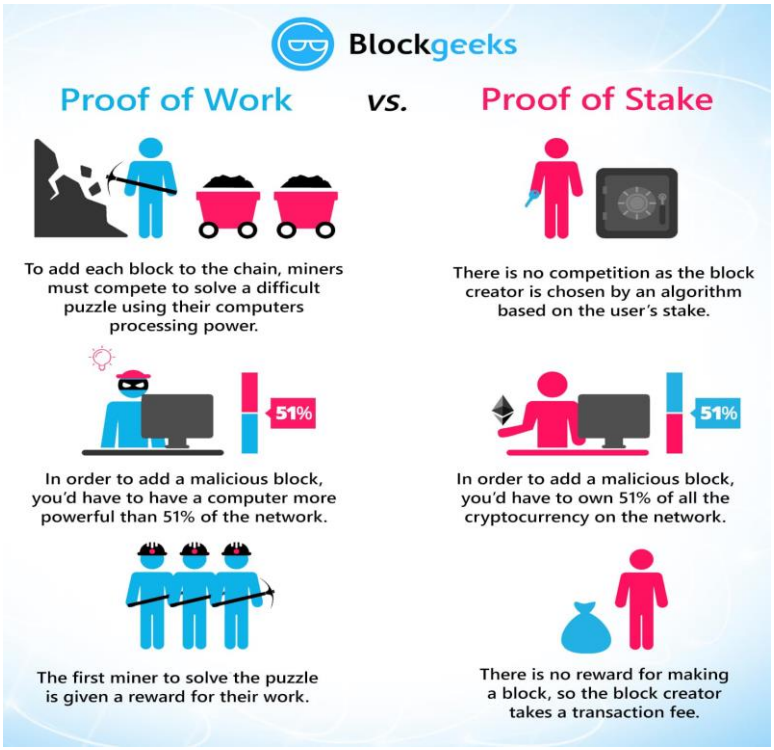


Figura 5. Comparativa PoW vs PoS. Fuente: blockgeeks.com

La puesta en común de estos dos consensos de minado es siempre que cada bloque de transacciones que se incorpora a la cadena sea correcto y legítimo.

2.3. BÚSQUEDA Y LECTURA DE TRANSACCIONES

2.3.1. ¿Cómo buscar una transacción?

Sabemos que las transacciones de criptomonedas pueden ser verificables, pues están guardadas en la Blockchain y solo tendríamos que consultarlo.

Para ello tendríamos que buscar a través de un explorador de bloques. Estos son el lugar en el que aparecen todas las transacciones que se han realizado en la cadena de bloques, siendo un comprendido general en el que se puede consultar todo el historial transaccional.

Podemos buscar en los siguientes exploradores:

-Bitcoin: blockchain.com y blockstream.

-Ethereum y ERC20: Etherscan y Ethplorer.

-Ripple: Bithomp y XRP Charts.

Existen más exploradores debido a que cada moneda o red Blockchain posee el suyo propio. Por ejemplo, no podríamos investigar transacciones de Bitcoin en un explorador de Ethereum y viceversa.

En estos exploradores podemos encontrar las diferentes transacciones de cualquier ID, así como sus saldos. En las direcciones se muestran todas las transacciones entrantes y salientes que se hayan producido en esa dirección, especificando el importe enviado, su destino y el tipo de tarifa que se pagó por ello. Al poder consultar todo el historial transaccional se puede localizar el primer bloque de la red, conocido como “bloque génesis”.

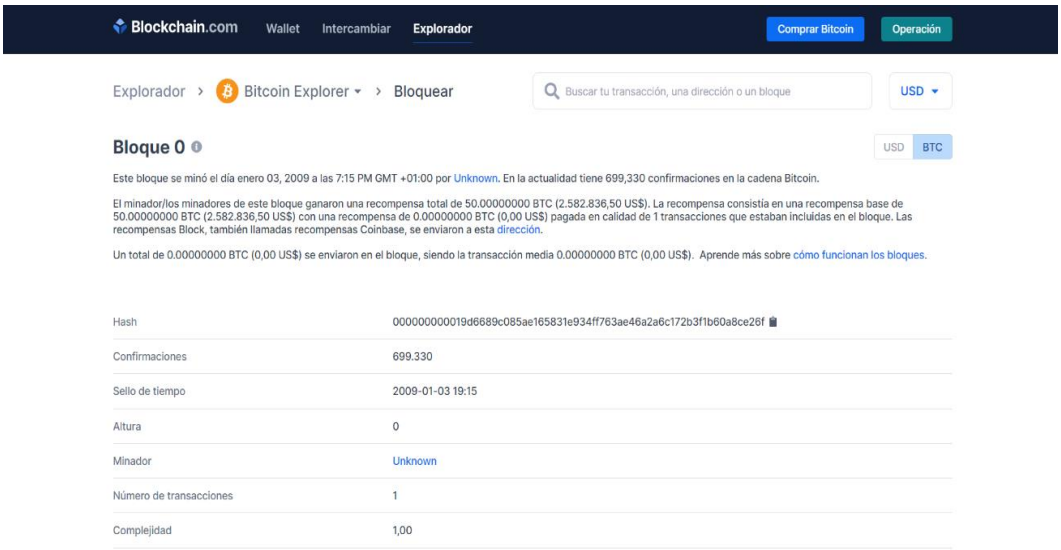


Figura 6. Bloque génesis de BTC. Fuente: blockchain.com

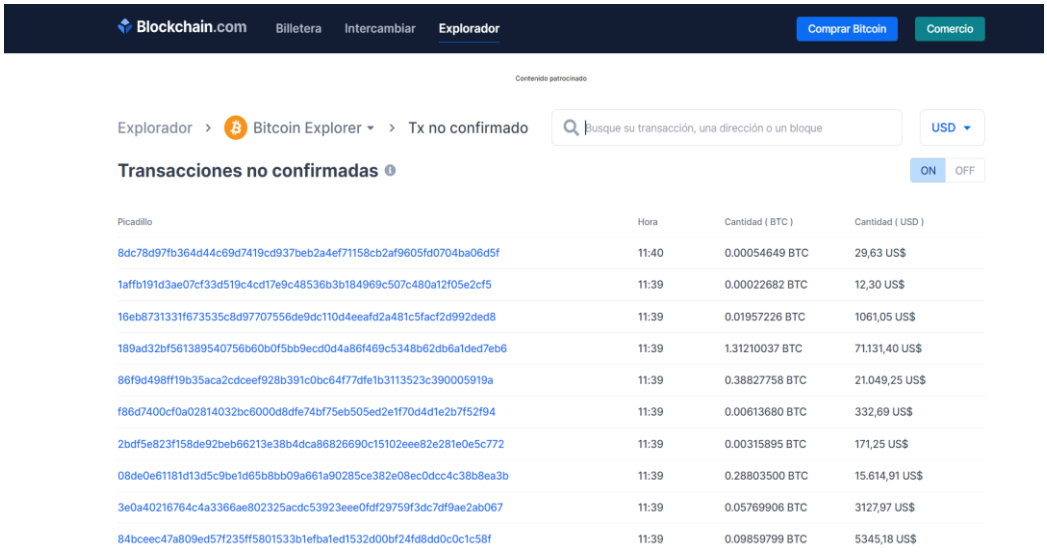


Figura 7. Transacciones de BTC enviadas, aún pendientes de confirmar, localizadas a través del explorador de bloques, el 21 de Abril de 2021. Fuente: blockchain.com

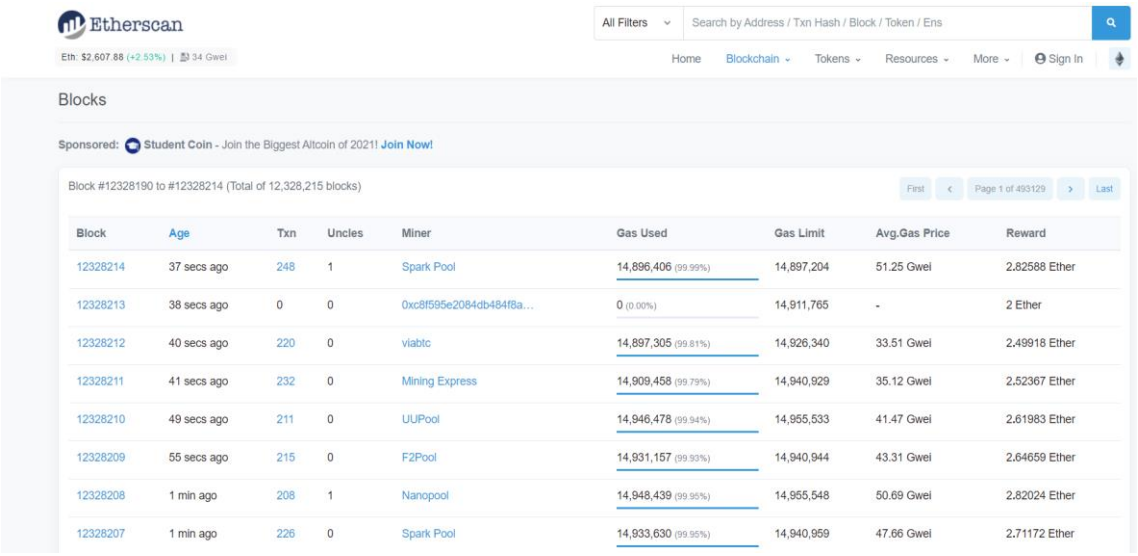


Figura 8. Bloques de Ether ya minados, localizados a través del explorador de bloques, el 28 de Abril de 2021. Fuente: etherscan.io

2.3.2. ¿Cómo leer una transacción?

Figura 9. Partes de una transacción. Fuente: Descubre Blockchain.

Una vez localizada la transacción que deseamos analizar podemos dividirla en cinco partes.

La primera es el **Hash**, conocido por ser el identificador de la transacción, es un algoritmo matemático que transforma una serie de datos en un código alfanumérico de longitud fija. Si queremos buscar los detalles de una transacción tendremos que ingresar este identificador en el buscador de bloques.

La segunda parte es la **dirección de envío**, no es más que la dirección que está enviando las criptomonedas así como la cantidad enviada.

La tercera es la "**fee**" de minería, tarifas que son pagadas a los mineros para que lleven a cabo el procesamiento de la transacción. Son pequeñas cantidades que se destinan a estimular la minería, ya que es un proceso fundamental para la seguridad y el funcionamiento de las criptomonedas, recompensando la labor de los mineros.

La cuarta parte son las **direcciones de recepción**, a las que se dirige la transacción con la cantidad de cada una.

La quinta parte es el **estado** en el que se encuentra la transacción, una vez emitida tiene que pasar todo el proceso hasta confirmarse, ya que esta puede ser cancelada por los mineros. El estado es de vital importancia para conocer si el intercambio se ha llevado a cabo.

2.4. CRIPTOGRAFIA Y DESCENTRALIZACIÓN

Las criptomonedas y el Blockchain se basan en dos conceptos, la criptografía y la descentralización.

Estos conceptos han existido durante años, pero han ido siendo cada vez de una mayor complejidad debido a los avances tecnológicos.

En los sistemas centralizados el mando es de una persona o conjunto de ellas, en el que los demás están sometidos a la autoridad de estos. El problema que encuentra este sistema es la falta de democracia y los problemas de seguridad que se pueden generar. Los fallos en sistemas centralizados pueden bloquear la red, ya que al caer el nodo central arrastra al resto de nodos impidiendo su funcionamiento.

Un sistema descentralizado el poder se divide entre todos los miembros, la ventaja de seguridad que este presenta este sistema es que es prácticamente imposible de abatir por un ataque malicioso, ya que para que este sea efectivo es necesario tener al menos un 51% del poder. La información de toda la red se encuentra repartida entre todos los participantes y si alguien desea realizar alguna acción ilegitima al realizarse una transacción, el resto de nodos pueden rechazarla, para esto es muy importante la confianza entre los participantes. Los fallos en uno de los nodos no impiden a los demás seguir trabajando.

Los cálculos que se siguen este tipo de sistemas son los siguientes:

Vamos qué ocurre si sucede un ataque malicioso en el sistema. Un atacante puede desear crear una cadena más rápido o de una forma no válida comparada con la cadena honesta. Los nodos no aceptaran el intercambio, invalidando el pago, por lo que no admitirán un bloque atacante.

La carrera entre una cadena honesta y una cadena maliciosa puede interpretarse como un Paseo Aleatorio Binomial. El suceso que progresa es la cadena honesta creando un

bloque, aumentado el liderato por +1 y siendo la cadena maliciosa la que fracasa, reduciéndose el espacio en -1.

La probabilidad de que se logre un ataque malicioso desde el déficit es similar al concepto estadístico de la Ruina del Jugador. Un jugador con crédito ilimitado comienza con un déficit y puede jugar potencialmente un número infinito de intentos para alcanzar el equilibrio, la probabilidad de que alcance ese punto la asociamos con que el ataque malicioso pueda alcanzar en algún momento la cadena honesta:

p = probabilidad de que un nodo honesto encuentre el siguiente bloque.

q = probabilidad de que el atacante encuentre el siguiente bloque.

qz = probabilidad de que el atacante alcance la cadena honesta, desde z bloques atrás.

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Figura 10. Probabilidad de que el ataque logre alcanzar la cadena honesta. Fuente: bitcoin.org

Con p > q, la probabilidad disminuye de forma exponencial a medida que aumenta el número de bloques que el ataque malicioso tiene que llegar a lograr. La oportunidad de lograr el ataque de va desapareciendo a medida que se va quedando atrás.

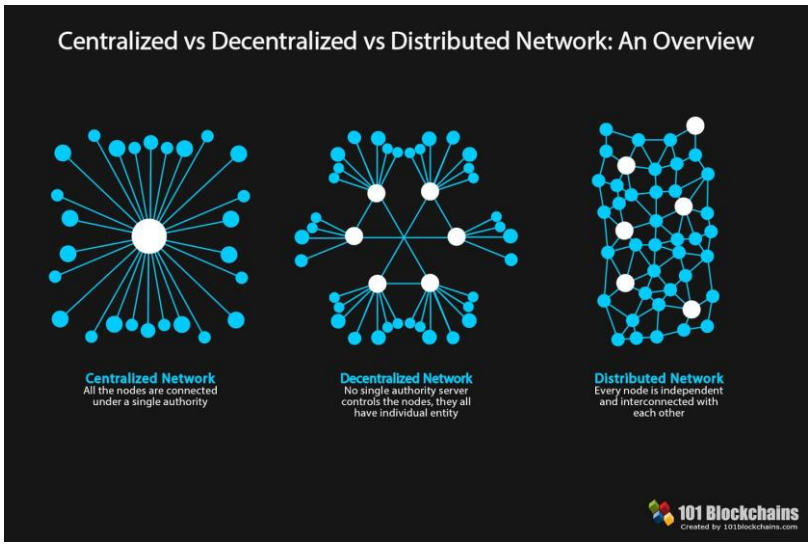


Figura 11. Tipos de redes. Fuente: 101 Blockchains.

Por lo que el dinero descentralizado presenta una serie de ventajas:

- La no intervención de terceros, con unos menores costes.

- Dinero depositado en cuentas en las que solo el usuario tiene acceso.
- Fácil acceso mediante dispositivos móviles.
- Bajas comisiones, únicamente por el minado al producirse las transferencias.
- Transacciones mucho más rápidas.
- Seguridad del sistema.

La **criptografía** es la otra cualidad sobre la que se rigen las criptomonedas, la cual existe desde hace miles de años, apareciendo referencias de cifrado en libros como *El antiguo testamento*.

La nueva criptografía basada en el cifrado con clave asimétrica surge con el diseño que idearon los dos criptógrafos estadounidenses; Martin Hellman y Whitfield Diffie. Crearon un nuevo tipo de algoritmo criptográfico basado en dos claves: una pública para cifrar y otra privada para descifrar. Con lo que para poder descubrir el contenido hace falta poseer ambas llaves.

El sistema permite saber quién envió la información debido a la clave pública pero que solo pueda acceder la información el poseedor de la clave privada.

Las criptomonedas utilizan la criptografía de clave asimétrica, con una variación que se fundamenta en curvas elípticas, logrando utilizar claves más cortas y manteniendo la misma seguridad. Las transacciones se reciben con una clave pública, de la que todos tienen información, mientras que la clave privada es utilizada para la firma de las transacciones.

Por lo que la criptografía permite la conservación de la información y la seguridad necesaria para la fiabilidad de las transacciones.

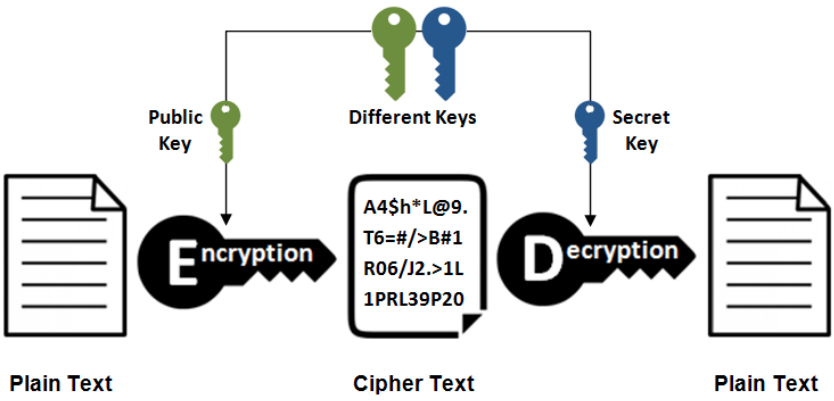


Figura 12. Esquema de criptografía asimétrica. Fuente: Medium.

En una transacción entre dos individuos, vamos a ver el tiempo necesario que puede esperar el receptor para obtener la seguridad necesaria de que el emisor no modifique el intercambio. Si el emisor que es el atacante, desea cambiar el pago para devolvérselo así mismo, el receptor recibirá una notificación del suceso, al que el emisor espera que ya sea tarde.

El receptor del intercambio crea un nuevo par de claves, dándole la clave pública al emisor poco antes de la firma, impidiendo que el emisor con un ataque malicioso pueda preparar una cadena de bloques con antelación.

Tras haberse emitido la transacción, el emisor atacante empieza a trabajar en secreto una cadena similar que tiene una versión alternativa de la transacción.

El receptor espera hasta que la transacción se añada al bloque y los z bloques se añadan al principal. Se desconoce el avance que lleva el atacante, pero contemplando que los bloques honestos han cogido la media de tiempo esperada por bloque, el posible progreso del atacante sigue estadísticamente la distribución de Poisson con valor esperado de:

$$\lambda = z\frac{q}{p}$$

Figura 13. Distribución de Poisson. Fuente: bitcoin.org

Si se quiere conseguir la probabilidad de que el atacante pueda llevar a cabo su deseo, se multiplica la densidad de Poisson para cada aumento en el progreso paralelo que ha llevado hasta ahora, por la probabilidad que podría haber alcanzado desde el punto:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Figura 14. Probabilidad de que el atacante cumpla su cometido. Fuente: bitcoin.org

Se debe modificar para así no sumar la cola infinita de la distribución:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Figura 15. Probabilidad de que el atacante cumpla su cometido. Fuente: bitcoin.org

Si se convierte en un lenguaje de programación C para verificar resultados:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z) {

double p = 1.0 – q;
double lambda = z * (q / p); double sum = 1.0; int i, k;
for (k = 0; k <= z; k++)
{

double poisson = exp(-lambda); for (i = 1; i <= k; i++)

poisson *= lambda / i;
sum -= poisson * (1 – pow(q / p, z – k));
}

return sum; }
```

Fuente: bitcoin.org

Resultados que se obtienen.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Figura 16. Resultados para q= 0.11 y para q= 0.3. Fuente: bitcoin.org

Vemos que en la probabilidad q=0.1 de que un atacante encuentre el siguiente bloque para una z=0, la probabilidad de que el nodo honesto conecte con el siguiente bloque es del 100%. Ante aumentos de la z se comprueba que se reduce la posibilidad de que el nodo honesto alcance el siguiente bloque.

Para q=0.3 y una z=5, la probabilidad de que el nodo honesto encuentre el siguiente bloque es mayor que para una q=0.1 con la misma z.

En P < 0,1%

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

Figura 17. Resultados para p < 0.001. Fuente: bitcoin.org

CAPÍTULO 3. ANALÍSIS INDIVIDUALIZADO DE CRIPTOMONEDAS.

A día de hoy existen miles de criptomonedas en el mercado y subiendo, cada vez hay más proyectos diferentes, nuevas monedas que aportan diferentes utilidades, con el objetivo de crearse su propio ecosistema con una comunidad detrás que lo apoye. En este capítulo vamos a ver algunas de las criptomonedas más reconocidas del mercado y las funcionalidades que están detrás de ellas.

Hay que mencionar primero un concepto básico de este entorno; se diferencia a la moneda líder, el Bitcoin (BTC), de las demás monedas que van surgiendo, denominadas "altcoins".

3.1. Bitcoin (BTC)

La primera y más importante de criptomonedas, número uno en capitalización de mercado, fue desvelada en el 2008 con la publicación del "White Paper" de Bitcoin y lanzada al año siguiente, bajo el seudónimo del creador, Satoshi Nakamoto. El lema de la moneda es "*Bitcoin: un sistema de dinero en efectivo electrónico "peer-to-peer".*

Desarrollada para usarse con la tecnología blockchain y con la criptografía, esta moneda presenta las características básicas de las criptomonedas; descentralizada, segura, finita (no todas), internacional, con pequeños costes de envió y sin terceros. Esta moneda sigue principalmente el mecanismo de consenso "proof of work" (PoW) en su red, lo que hace posible el peer-to-peer.

Para que el Bitcoin tuviera valor económico tuvo que seguir reglas económicas como la ley de oferta y demanda, ya que esta moneda es limitada y escasa (21 millones de monedas). El proceso "halving" es el encargado de regular la oferta, además, la solo existencia de 21 millones de monedas hace que al aumentar la demanda, el precio también lo haga. La escasez de bitcoins no será un problema en el caso de que pueda llegar a usarse por toda la población mundial ya que es capaz de dividirse hasta en un octavo y puede que en aún más en el futuro.

Se han creado bifurcaciones a través de la Blockchain de Bitcoin. Una de ellas es Bitcoin Cash (BCH), en agosto de 2017 aparece con el objetivo de resolver los problemas de escalabilidad que estaba presentando Bitcoin en aquel entonces: tardanza en las verificaciones y aumentos en los costes de transacción. En los últimos años Bitcoin mejoró su escalabilidad con una red de pagos rápidos llamada Lighting Network, dejando esta bifurcación de BCH en tierra de nadie y sin objetivo aparente.

Bitcoin Cash también sufrio un proceso de bifurcación, en noviembre de 2018 se creó Bitcoin SV (BSV), con mucha polémica y con el objetivo principal de devolver la esencia al Bitcoin como medida de pago electrónica.

3.2. Ethereum (ETH)

La segunda criptomoneda en capitalización de mercado y junto al Bitcoin la más potente, es una plataforma de código abierto, descentralizada, que funciona como plataforma para otras criptomonedas, así como para la creación de contratos inteligentes y dapps. Esta plataforma trabaja con la moneda llamada “ether”, que se usa para recompensar a los que participan en el modelo de consenso.

La idea surgió en el 2013 bajo un documento técnico escrito por el programador ruso Vitalik Buterin, tras comprobar algunas limitaciones en el Bitcoin, logro a través de una nueva capa de programación crear el token,“ether”.

El withepaper escrito fue titulado, *“A Next Generation Smart Contract & Decentralized Application Platform”*, en 2015 se lanza definitivamente, proyectando por primera vez una ICO. Ethereum tiene un total de 8 cofundadores.

En 2016 se lanza la primera DAO, una empresa de gestión automatizada y descentralizada en torno a los contratos inteligentes. Tras un fallo de la DAO, se produjo una sustracción de 3 millones de ETH, por lo que la solución que se impuso fue realizar un *hardfork*, dividiéndose en dos líneas de Blockchain; Ethereum (ETH) y Ethereum Classic (ETC).

La principal cualidad que aporta Ethereum es la creación de una plataforma que permite elaborar contratos inteligentes con la tecnología Blockchain.

3.3. Ripple (XRP)

Esta moneda es respaldada por la empresa Ripple Labs, compañía fundada en 2012 por Chris Larsen y Jed McCaleb, afianzada como un protocolo de pagos único en 2015. La moneda se diseña como una solución a los inconvenientes de las transferencias interbancarias e internacionales, que usan la red SWIFT debido a su coste y lentitud. Son responsables de establecer una blockchain que posibilita crear uno de los sistemas de pagos más eficientes del mundo, además se considera al protocolo Ripple como complementario al sistema bancario actual.

Lo que diferencia XRP de otras criptomonedas es su centralización en torno a la empresa Ripple Labs, siendo la empresa capaz de imposibilitar direcciones, bloquear activos o manipular emisiones, además la mayor parte de los tokens están en propiedad de la empresa creadora. La centralización de la moneda ocurrió desde su creación ya que Ripple creo 100 millones de XRP y son los existentes a día de hoy, habiéndose emitido en torno a 46 millones.

En cuanto a su funcionamiento, esta moneda no se mina, utiliza la tecnología DLT con su propio protocolo de consenso (RPCA), lo que les vale para cotejar las transacciones que se hacen dentro del sistema de RippleNet.

3.4. Litecoin (LTC)

Creada por Charlie Lee un ex trabajador de Google, el Litecoin es el hermano pequeño del Bitcoin, la visión de Charlie era crear una versión “lite” de este, comparándose siempre entre ambas como el oro y la plata. Esta moneda surge en 2011 como alternativa al Bitcoin, utilizando su mismo código fuente, a diferencia de que las transacciones con LTC son más rápidas y económicamente menos costosas, debido a que el proyecto se orienta al eCommerce, por lo que esta moneda es una alternativa eficiente al Bitcoin.

En funcionamiento, utiliza el protocolo de PoW, y como la mayor parte de las criptomonedas que utilizan este algoritmo la cantidad de LTC aumenta progresivamente con cada bloque extraído.

Cualidades de Litecoin que le diferencian de su hermano mayor; la red procesa un bloque cada 2,5 minutos (cada 10 en Bitcoin), siendo la red cuatro veces más veloz. La Blockchain es bastante ligera ya que el peso medio de los bloques es de 65KB. El proceso de halving en LTC es cada 840.000 bloques (cada 210.000 en BTC), estando actualmente las recompensas para los mineros en 12.5 LTC. La masa monetaria límite es de 84 millones de LTC (21 milones en BTC). En cuanto a la escalabilidad, uno de los problemas de Bitcoin, Litecoin lo mejora, ya que soporta un máximo de 56 transacciones por segundo (máximo 7 en Bitcoin). Estas cualidades hacen que la velocidad en las transacciones y el atractivo de minería sea mayor en Litecoin, además de tener unas tarifas de transacción extremadamente bajas.

3.5. EOS (EOS)

Plataforma desarrollada por Daniel Larimer y Brendan Blumer de la empresa Block.one, es el principal rival de Ethereum, se centra en la construcción de aplicaciones descentralizadas, buscando que los programadores utilicen su tecnología Blockchain y que el uso de esta red sea más fácil y cómoda de usar que la de los competidores. Su arquitectura de Blockchain permite millones de transacciones por segundo, para permitir

un despliegue rápido de aplicaciones descentralizadas, por lo que la tiene mayores niveles de escalabilidad que la competencia.

Actualmente hay 955 millones de EOS en circulación y un suministro total de 1.03 mil millones de tokens.

3.6. Binance Coin (BNB)

Binance es uno de los exchanges más importantes del mundo, su fundador Changpeng Zhao lanzó al mercado la criptomoneda BNB en Julio de 2017. El token basado en Ethereum se crea para brindar ventajas a los consumidores cuando realizan las transacciones, la utilidad que ofrece se centra en la aplicación de rebajas hasta del 50 por ciento cuando se realizan transacciones internas dentro del Exchange de Binance, otorgándoles a los poseedores de la moneda descuentos en las comisiones.

Además BNB es una de las monedas más rápidas del mercado ya que puede soportar alrededor de 1.5 millones de transacciones por segundo.

Se emitieron 200 millones de BNB que se irán reduciendo hasta llegar a las 100 millones de monedas.

3.7. Monero (XRM)

Esta criptomoneda destaca por su privacidad. Creada con código abierto en abril de 2014 por un equipo de desarrolladores, es una bifurcación de Bytecoin. Totalmente enfocada a la seguridad de su anonimato, la privacidad y la descentralización, todas las operaciones con XRM son totalmente anónimas, incluyéndose la IP de los participantes de la transacción, por lo que los únicos conocedores de la información de la transacción son los dos participantes de ella. En criptos como Bitcoin, se considera la red como seudoanónima, debido a que los movimientos transaccionales de Bitcoin son públicos y se puede llegar a establecer una cierta relación, algo que en Moreno es inviable siendo imposible de rastrear. Para poder lograr este nivel de privacidad Monero ha utilizado criptografía avanzada.

Por este nivel de privacidad la moneda es comúnmente utilizada para la realización de pagos en actividades ilícitas en la *Deep Web.*

Monero pasó de utilizar el algoritmo de minería CryptoNight al de RandomX en la actualidad, permitiendo solo la minería por CPU de ordenadores domésticos y evitando la minería con tarjetas gráficas o ASIC (hardware).

3.8. Cardano (ADA)

Fundada por uno de los creadores de Ethereum, Charles Hoskinson, la red Cardano es una plataforma de tercera generación, parecida a ETH en el ámbito de los contratos inteligentes, y que utiliza el token ADA.

El proyecto de código abierto utiliza la prueba de participación (PoS) concretamente el algoritmo de consenso Ouroboros, cuyo principal reclamo es la escalabilidad y la alta velocidad que posee la Blockchain. Busca solucionar problemas de escalabilidad de plataformas más grandes en el terreno de los "Smart Contracts" como Ethereum, mejorar la descentralización y la seguridad tecnológica de la red, haciendo que se considere a Cardano como una Blockchain de tercera generación.

A fecha de Septiembre de 2021 Cardano es la tercera moneda por capitalización de mercado siendo una de las más reconocidas del ecosistema.

3.9. Stellar (XLM)

Nacida en julio de 2014 y basada en el protocolo de Ripple Labs tras una bifurcación, es una red abierta la cual posibilita mover y guardar dinero. En primera instancia la misión de Stellar fue dar acceso al mundo financiero a personas excluidas de él, cambiando sus prioridades hacia ayudar a empresas financieras a interconectarse gracias a la tecnología de la cadena de bloques.

La red ofrece servicios financieros a bajo coste mediante la moneda Stellar Lumens (XLM), además de unas operaciones rápidas y seguras. El objetivo de la organización creada por Jed McCaleb y Joyce Kim ex trabajadores de Ripple es convertirse en la banca del futuro, ya que con la plataforma podrán poseer una cuenta bancaria en un organismo financiero, hacer envíos a muy bajo coste, transferencias de dinero en segundos con dispositivos móviles y todo con una alta seguridad debido a la tecnología Blockchain.

3.10. IOTA (MIOTA)

Es un libro mayor de contabilidad distribuido, de código abierto, donde el objetivo es poder intercambiar información y valor de forma segura en internet. La principal particularidad de IOTA es que no utiliza la tecnología Blockchain, sino que emplea su propia tecnología llamada "Tangle", la cual se basa en un concepto matemático llamado "grafo acíclico dirigido" (DAG) un tipo de sistema de nodos que confirman las transacciones. Esta plataforma brinda unas velocidades mucho mayores que las cadenas de bloques tradicionales.

De las ventajas de la red de IOTA es la no existencia de comisiones, ya que al no haber blockchain no hay minería, además de tener una fácil escalabilidad.

La Fundación IOTA posee cuatro cofundadores y tiene su sede central en Alemania, con un buen futuro por delante gracias a su tecnología, trabaja con empresas destacadas como: Orange, Jaguar, Land Rover, Volkswagen, Bosch, con la visión de crear un mercado descentralizado donde se puedan comerciar flujos de datos.

3.11. Tether (USDT)

Una criptomoneda diferente, de las conocidas como “stablecoin”, ya que se vincula con el dólar estadounidense, replicando su precio. El USDT funciona como token de segunda capa sobre otras cadenas de bloques como Bitcoin, Ethereum, EOS, Tron…. Es emitida por la empresa Tether Limited, donde la conexión del token con el dólar se consigue mediante el sustento de una suma de papel comercial, depósitos fiduciarios, efectivos y letras de tesoro en reservas, siendo el valor en USD igual a la cantidad de USDT en movimiento.

El objetivo de su creación es juntar la naturaleza sin límites de las criptomonedas con el respaldo de un valor, en este caso el dólar. Su principal característica es la nula correlación con el resto de criptos, cubriéndose el precio ante los momentos de caídas en el mercado y limitando la volatilidad que presentan comúnmente las criptomonedas.

CAPÍTULO 4. NUEVAS FORMAS DE FINANCIACIÓN EMPRESARIAL A TRAVÉS DE CRIPTOMONEDAS.

A la hora de echar a andar un proyecto es necesario tener una serie de recursos económicos para que este pueda funcionar. Cada vez son más los negocios que se inician por iniciativa propia y por tanto cada vez hay más diferentes opciones para financiar la puesta en marcha de una nueva empresa, desde los métodos de financiación más clásicos a otros que han ido apareciendo en los últimos años: líneas de crédito, préstamos bancarios, ayudas públicas, OPV, factoring, leasing, crowdfunding, Business Angels, capital de riesgo, etc…. La tecnologia Blockchain y las criptomonedas han causado diferentes formas de recaudación de capital para las empresas. Esta variedad de alternativas permite a cada empresario adaptarse a la financiación que convenga más adecuada para su proyecto.

4.1. ICO

Las Initial Coin Offerings son un nuevo tipo de financiación asociado a las criptomonedas. Este método es usado para financiar “startups” en el mundo del blockchain, emitiendo las criptos a un precio fijado.

Proyectos del ecosistema como Ethereum, que recaudo 18 millones de dólares con una ICO o proyectos como IOTA (más de 400.000$) y NEO (556.500$) son ejemplos de empresas que han buscado este tipo de financiación para obtener un capital inicial para su desarrollo.

Para el lanzamiento de una ICO, los creadores del proyecto presentan el White Paper a los inversores, donde se encuentran todos los aspectos del mismo, financieros, publicitarios, miembros, desarrollo tecnológico y los caminos por los que se moverá el proyecto. Los emprendedores ofrecen a los inversores los tokens al precio de salida a cambio del dinero de la inversión. Para la recaudación de capital en esta en este periodo, se establece una fecha inicial y una final, que será la duración de la ICO. Desde el punto de vista del inversor, lo que busca es una revalorización con el tiempo del precio de los tokens iniciales que adquirió con la inversión, por lo que es de vital importancia creer realmente en el proyecto y hacer previamente un estudio del mismo. Hay que tener en cuenta el ratio riesgo/ganancia ya que este puede ser muy elevado, una inversión ganadora en el mercado de las ICO puede ser realmente complicada debido a su carácter novedoso y la escasa e incierta regulación que existe. A pesar de esto, una ICO que presente un gran potencial y su proyecto salga satisfactoriamente adelante puede presentar una rentabilidad al inversor nunca antes vista en otro tipo de mercados debido al carácter tan volátil. Un ejemplo puede ser Ethereum, al celebrarse la ICO en verano de 2014 el precio del token se encontraba en 0,311$, actualmente el precio es de 3120,23$, habiendo alcanzado un máximo histórico de 4372$.

Otro aspecto de las ICO es que los inversores no tienen derechos de decisión sobre la empresa, ya que son figuras jurídicas que están formadas antes de salir al mercado. Aunque hay casos en los que los inversores que poseen tokens pueden tener la posibilidad direccionar el proyecto si este se forma como una DAO, son un tipo de estructura especial dentro del ecosistema de las criptomonedas. Capacita a los dueños de los tokens a poder tomar decisiones sobre el desarrollo de la empresa, mediante sistemas democráticos de votación).

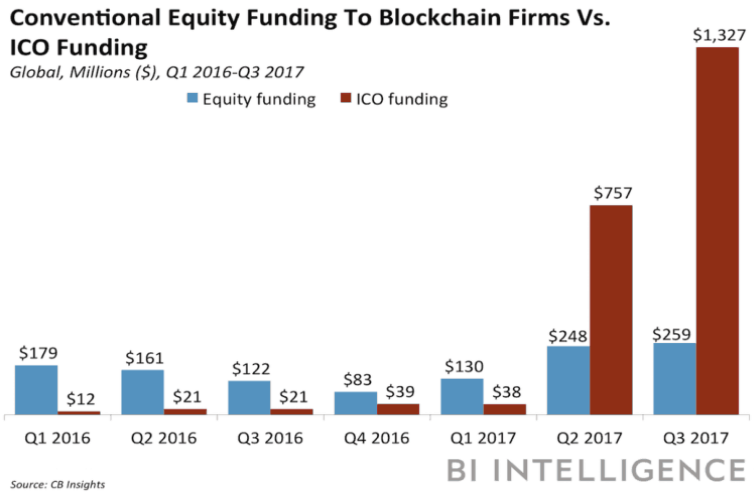


Figura 18. Momento en el que la financiación con ICO supera a los métodos de financiación tradicionales. Fuente: CB Insights.

Figura 19. Primer "boom" de financiación a través de ICO en millones de dólares. Fuente: Statista.

4.2. STO

Las Security Token Offerings se presentan como una nueva idea que recoja lo mejor de las ICO fusionado con las OPV de salida a bolsas tradicionales. Ante el riesgo y la poca regulación de las ICO, las STO aporta al inversor mayor transparencia y seguridad.

Las STO tendrán que cumplir las mismas obligaciones que una empresa que quiera salir a la bolsa pública. También se ofrecerán a los inversores y poseedores de los tokens dividendos de los beneficios de la empresa que haya realizado la STO. Del ámbito de las ICO aguarda la utilidad del Blockchain para brindar un sistema más claro y eficiente que el método actual que se emplea en los mercados de acciones. Tendrán una serie de regulaciones legales que no poseen las ICO, tanto para el inversor como para el desarrollador, se pedirá más información como: registros contables públicos, control de autoridades financieras y otros elementos propios de empresas que cotizan en bolsa. Se diferencian en que las ICO ofrecen un "utility token" para un uso en plataformas y las STO ofrecen un "security token", es decir, un valor fungible y comerciable que posee un cierto valor dentro del sector financiero.

Al igual que en las ICO el poder de decisión de los inversores al poseer los tokens dependerá únicamente de si el proyecto está constituido como una DAO.

4.3. IEO

Initial Exchange Offering, calificadas como las ICO de segunda generación. Las IEO tienen el mismo objetivo que las ICO, cambiando únicamente las formas. Estas se basan en la recaudación de capital con usuarios y fondos de un intercambio en concreto.

La forma en la que se presentan las IEOs es mediante los exchanges, siendo estos los encargados de estudiar y garantizar el proyecto. Los exchanges se encargan de la recolección de capital para la "startup" que busca lanzar el proyecto. La ventaja principal de esta medida de financiación es que ofrece una seguridad de que los proyectos que se lanzan son factibles y cuentan con un respaldo de confianza, además de la publicidad que les puede proporcionar la plataforma de intercambio.

La primera IEO fue creada por el conocido Exchange de Binance y tras ello muchos exchanges ofrecen la posibilidad a sus usuarios de poder hacerlo.

Este método de financiación se diferencia de las ICO en varios puntos: Las IEO son centralizadas, esto es debido a que todo está inspeccionado por el exchange y los dueños del proyecto. Se deben cumplir las exigencias que plantee la plataforma, además de un MVP. En una IEO al contrario que en con una ICO, garantiza que el token pueda comerciarse en el exchange, algo que en la ICO puede no darse nunca o que tarde un cierto tiempo. En el tema de la seguridad las IEO se llevan otro punto a positivo, en las ICO cualquiera puede comercializar con tokens y es algo que puede llevar a la realización de actividades ilegales, en cambio en las IEO hay que pasar el filtro KYC/AML para poder participar en ella, aunque dependiendo el tipo de perfil del inversor puede ser contraproducente tener que dar su información y preferir actuar desde el anonimato.

CONCLUSIONES

Durante el trabajo se ha ido desarrollando el ámbito de las criptomonedas, desde los primeros instantes en el que criptógrafos se plantearon la posibilidad de crear dinero virtual y descentralizado hasta la más actualidad.

Se ha visto las características que estás criptomonedas poseen, unas cualidades distintas a los métodos de cambio más tradicionales como es el dinero FIAT. Con estas particularidades se ha buscado crear un dinero rápido, que no esté controlado por terceras personas y que además aporte la seguridad suficiente como para creer en él.

Existen miles de proyectos por los que apostar, cada uno ofrece diferentes funcionalidades o trata de mejorar a sus competidores, esta amplia gama ofrece un mayor atractivo de estas monedas. Distintas velocidades de transacción, escalabilidad, forma de minado, seguridad, smart contracts…

Quiero mencionar en lo referente a la forma de validar las transacciones mi posición a favor hacia la PoS, visto durante el trabajo las formas en las que se minan los envíos considero que la PoS ofrece la misma seguridad que la PoW solo que de una forma mucho más saludable para el medio ambiente. Con los problemas de cambio climático que ya existen en el mundo, generar más consumo energético como el que necesita la PoW para funcionar es totalmente innecesario.

Por parte de las nuevas formas financiación que han experimentado un crecimiento notable en los últimos años, se pueden considerar unas opciones atractivas para empresas emergentes ya que pueden ofrecer unas rentabilidades muy altas comparado con métodos más tradicionales. Pero en cambio, la volatilidad de estas en su mercado

particular hace que estas inversiones sean muy arriesgadas, debido a la especulación en la compra de criptomonedas.

En cuanto a la tecnología Blockchain en la que se basan las criptomonedas, cabe destacar el futuro que presenta. Durante el trabajo se ha descrito la forma en la en la que las criptomonedas se mueven por la cadena de bloques a la hora de realizarse las transacciones, pero esta tecnología será de un uso eficaz en los próximos años para más ámbitos que el de las monedas digitales como: contratos inteligentes, productos financieros, comercio electrónico, almacenamiento de información…

Como conclusión final y desde mi punto de vista considero que las criptomonedas tienen potencial para convertirse en un método de pago para las personas en su día a día, pero en vez de sustituir el dinero FIAT, estas pueden verse como un complemento adicional a la hora de realizarse transacciones. Eso sí, se tendrán que aclarar ámbitos como el legislativo para que haya un consenso entre los países de todo el mundo a la hora producirse intercambios o ganancias patrimoniales con estas monedas, ya que como se sabe gozan de internacionalidad. Por último término afirmando que la tecnología Blockchain sin duda revolucionara el mundo en diferentes áreas llegando a asentarse en nuestras vidas más pronto que tarde.

Animo a toda la gente que sienta curiosidad por este mundo a investigar e interesarse por estas monedas virtuales.

BIBLIOGRAFÍA

- BUTERIN, V. 2013. A Next-Generation Smart Contract and Decentralized Application Platform. [online] Disponible en: https://ethereum.org/en/whitepaper/
- BBVA NOTICIAS. 2021. *11 formas de financiar un proyecto*. [online] Available at: <https://www.bbva.com/es/11-formas-de-financiar-un-proyecto/> [Accessed 6 August 2021].
- BBVA NOTICIAS. 2021. *11 formas de financiar un proyecto*. [online] Available at: <https://www.bbva.com/es/11-formas-de-financiar-un-proyecto/> [Accessed 16 August 2021].
- Bit2Me Academy. 2021. *¿Qué es el bloque génesis (Genesis Block)? de Bitcoin | Bit2Me Academy*. [online] Available at: <https://academy.bit2me.com/que-es-bloque-genesis/> [Accessed 13 May 2021].
- Bitcoin forum. 2010. *Pizza for bitcoins?.* [online] Available at: <https://bitcointalk.org/index.php?topic=137.0> [Accessed 12 July 2021].
- Blockgeeks. 2021. *Blockchain Community and Education*. [online] Available at: <https://blockgeeks.com/> [Accessed 6 August 2021].
- Champagne, P., 2018. *El Libro de Satoshi*. [ebook] Edición BlockchainEspana.com. Available at: <https://libroblockchain.com/wp-content/uploads/2018/07/Libro-de-Satoshi-Blockchain-Espana-v1-junio-2018.pdf> [Accessed 10 May 2021].
- CNMV. 2021. *Criterios en relación con las ICOs*. [ebook] Comisión Nacional del Mercado de Valores, pp.1-4. Available at: <https://www.cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf> [Accessed 16 August 2021].

- CoinMarketCap. 2021. *Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap*. [online] Available at: <https://coinmarketcap.com/> [Accessed July and August 2021].
- Cointelegraph. 2021. *Qué es DAO y cómo funciona*. [online] Available at: <https://es.cointelegraph.com/ethereum-for-beginners/what-is-dao> [Accessed 13 July 2021].
- Criptotario.com. 2021. *Prueba de trabajo vs prueba de participación*. [online] Available at: <https://criptotario.com/prueba-de-trabajo-vs-prueba-de-participacion> [Accessed 18 July 2021].
- Grigg, I., 2017. *EOS - An Introdution*. [whitepaper] p.12. Available at: <https://www.iang.org/papers/EOS_An_Introduction-BLACK-EDITION.pdf> [Accessed 12 July 2021].
- Kiayias, A., Rassell, A., David, B. and Oliynykov, R., 2021. *Ouroboros: A probably security oriif-of stake Nlockchain Protocol*. [whitepaper] pp.1-54. Available at: <https://whitepaperdatabase.com/cardano-ada-whitepaper/> [Accessed 26 July 2021].
- Lara, A., 2020. *Blockchain & Criptomonedas*. 1st ed. Italia: Amazon, pp.22-202.
- Lee, C., 2011. *Litecoin Whitepaper*. [whitepaper] p.4. Available at: <https://whitepaper.io/coin/litecoin> [Accessed 11 July 2021].
- Mazieres, D., 2014. *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. [whitepaper] Stellar Develpoment Fundation, pp.1-32. Available at: <https://www.stellar.org/papers/stellar-consensus-protocol> [Accessed 27 July 2021].
- Nakamoto, S., 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Whitepaper] p.9. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 10 July 2021].
- Partz, H., 2020. *¿Cómo se usa un explorador de bloques?*. [online] Cointelegraph. Available at: <https://es.cointelegraph.com/news/how-do-you-use-a-block-explorer> [Accessed 13 May 2021].
- Pierce, B., Collins, R. and Sellars, C., 2014. *Tether: Fiat currencies on the Bitcoin blockchain*. [whitepaper] p.20. Available at: <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf> [Accessed 13 July 2021].
- Pierce, B., Collins, R. and Sellars, C., 2014. *Tether: Fiat currencies on the Bitcoin blockchain*. [whitepaper] p.20. Available at: <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf> [Accessed 30 July 2021].
- Popov, S., 2018. *The Tangle*. [whitepaper] pp.1-28. Available at: <https://www.allcryptowhitepapers.com/iota-whitepaper/> [Accessed 28 July 2021].
- Rodriguez, F., 2018. *Blockchain & Criptomoneda*. [ebook] FINANCE CORPORATION, p.63. Available at: <https://books.apple.com/us/book/blockchain-y-criptomoneda/id1342781792> [Accessed 7 May 2021].
- Schwartz, D., Youngs, N. and Britto, A., 2018. *The Ripple Protocol Consensus Algorithm*. [whitepaper] pp.1-8. Available at: <https://ripple.com/files/ripple_consensus_whitepaper.pdf> [Accessed 14 July 2021].
- Tapscott, D. and Tapscott, A., 2017. *Blockchain Revolution*. 1st ed. Barcelona: Grupo Planeta, pp.23-88.
- Torres, J., 2019. *Criptomonedas. Qué son, cómo utilizarlas y por qué van a cambiar el mundo.* 2nd ed. Barcelona: Grupo Planeta, pp.21-188.
- Van Saberhaen, N., 2014. *Cryptonote v 2.0*. [whitepaper] MONERO – Private Digital Currency, pp.1-20. Available at: <https://www.allcryptowhitepapers.com/monero-whitepaper/> [Accessed 20 July 2021].

- Vazquez, A., 2018. *¿Qué son las funciones Hash y para que se utilizan? | CYSAE LEGAL*. [online] CYSAE- Abogados Legaltech Madrid. Available at: <https://www.cysae.com/funciones-hash-cadena-bloques-blockchain/> [Accessed 18 May 2021].
- Vega, G., 2021. El primer tuit de la historia, vendido por 2,9 millones de dólares. *El País*, [online] Available at: <https://elpais.com/tecnologia/2021-03-23/el-primer-tuit-de-la-historia-vendido-por-29-millones-de-dolares.html> [Accessed 30 August 2021].
- Zhao, C., 2017. *Binance Exchange*. [whitepaper] pp.1-17. Available at: <https://www.exodus.com/assets/docs/binance-coin-whitepaper.pdf> [Accessed 16 July 2021].