GRADO EN COMERCIO

TRABAJO DE FIN DE GRADO

"LAS CRIPTOMONEDAS Y LA RED BLOCKCHAIN.

PROYECTO PARA LA CREACIÓN DE UNA CRIPTOMONEDA EN LA FACULTAD DE COMERCIO DE VALLADOLID."

LUCAS IZQUIERDO LATORRE

FACULTAD DE COMERCIO

VALLADOLID, 2021

UNIVERSIDAD DE VALLADOLID

GRADO EN COMERCIO

CURSO ACADÉMICO 2020-21

TRABAJO DE FIN DE GRADO

"LAS CRIPTOMONEDAS Y LA RED BLOCKCHAIN.

PROYECTO PARA LA CREACIÓN DE UNA CRIPTOMONEDA EN LA FACULTAD DE COMERCIO DE VALLADOLID."

Trabajo presentado por: Lucas Izquierdo Latorre

Firma:

Tutor: Francisco Javier Galán Simón

Facultad de comercio

Valladolid 2021

ÍNDICE

Listado de imágenes

1 Introducción

"La más larga caminata comienza con el primer paso"

Bien es sabida la velocidad a la que, en estos tiempos, avanzan los medios tecnológicos adaptándose continuamente a las cambiantes necesidades del ser humano. Así observamos continuas actualizaciones, no solo en los dispositivos y herramientas que utilizamos, sino también -y con mayor importancia- en la forma en que nos comunicamos e interaccionamos en sociedad. Es gracias a ello que hemos desarrollado ingeniosos sistemas informáticos para ayudarnos con estas necesidades de acción recíproca entre personas

Como era de esperar, también estas innovaciones han tenido lugar en el sector financiero con nuevos medios de pago y de manejo de valor que empleamos en nuestro día a día. El "dinero" también es una parte fundamental de las funciones sociales y de motivación en la colaboración entre individuos.

Para entender su historia debemos remontarnos muchos siglos atrás, cuando las personas empleaban el trueque como medio de intercambio de los productos obtenidos de su trabajo. En aquella época se consideraba "dinero" a cualquier objeto de valor susceptible de convertirse en forma de pago a cambio de bienes o servicios. Más tarde, la aparición de las primeras monedas surgió como consecuencia de la necesidad de ajustar esos intercambios haciendo más sencillo establecer un precio para cada producto.

A lo largo de la historia el material principal que se ha empleado para la creación de monedas ha sido el oro, pero ¿Por qué? El oro tiene varias características muy interesantes para ser empleado como moneda de cambio, en primer lugar, es su existencia limitada, a diferencia de otros metales que podemos encontrar en relativamente grandes cantidades, esto le confiere un valor especial. Gracias a esta limitación, el oro mantiene un valor estable lo que hace que independientemente de quien gobierne, este mantendrá su valor inalterado.

Muchos años después, en el s. IX, hizo su aparición el "papel moneda" con la intención de facilitar aún más los intercambios al no ser necesario transportar grandes cantidades de monedas para hacer los intercambios, tanto el papel moneda como las propias monedas han mantenido un respaldo en oro durante

mucho tiempo, esto significaba que por cada billete o moneda que se creaba, había una cantidad de oro equivalente, independientemente de que ese billete o esa moneda estuvieran confeccionados en otro material y requirieron de un largo proceso de aceptación entre la gente al valerse de la confianza de éstos para ser posible su uso sin necesidad de respaldarse en el oro. Así apareció el conocido como dinero fiduciario (basado en la fe).

Si continuamos avanzando hasta mitad del siglo pasado nos encontramos por fin con la primera aparición de las tarjetas de crédito el conocido como “dinero de plástico”, que Frank McNamara tras un infortunio en un restaurante en el que a la hora de pagar la cuenta descubrió que había olvidado su cartera, decidió crear una tarjeta que le identificaba para realizar pagos en diversos establecimientos: la Dinners´ Club. En sus inicios, solo era aceptada en unos pocos restaurantes que confiaban en él, pero para finales de ese mismo año ya era empleada por más de 20.000 personas.

Pero la historia no acaba aquí, como recientemente hemos podido comprobar, las entidades bancarias y el modo en el que realizamos nuestros pagos también han avanzado a un ritmo vertiginoso, gracias a la implementación de los nuevos sistemas de banca online o incluso la eliminación de tarjetas de crédito físicas a favor del pago mediante los teléfonos móviles o incluso relojes inteligentes. Con el implacable avance de la globalización y la digitalización, nuevas formas de pago y de realizar transacciones han aparecido para quedarse, nuevos medios que además de buscar optimizar la velocidad y costes, también aseguran la seguridad en cada transacción que hagamos.

Con todo esto, podemos afirmar que el dinero, da igual en que medio sea representado, ostenta su valor gracias a la confianza. Mientras se logre una aceptación por parte de los usuarios, somos libres de desarrollar nuevos medios cada vez más avanzados para desenvolver ese papel.

RESUMEN

Este trabajo final pretende explicar de forma sencilla y accesible cómo funciona la tecnología del blockchain y su aplicación al mundo de las criptomonedas. Así cómo su modo de funcionamiento, qué interés pueden suscitar y por qué son tan importantes en la sociedad financiera actual.

Es un tema extenso y técnicamente complejo que pretendo acotar abordando los aspectos fundamentales y prácticos que describen el mecanismo tanto de uso, como de desarrollo de las criptomonedas sin entrar en los complicados entresijos de cómo funcionan sus códigos, pues precisan de conocimientos avanzados de matemáticas, informática y criptografía.

Está desarrollado en dos partes diferenciadas. Una primera parte donde se trata la conceptualización e la información básica del tema tratado, además de algunos de los proyectos de criptomonedas más interesantes en la actualidad y sus nuevas aplicaciones descentralizadas y Smart contracts. En la segunda parte, se realiza una aplicación práctica basada en la creación de una criptomoneda -de la forma más sencilla que he podido acertar- con el fin de proporcionar un token propio a la Facultad de Comercio de Valladolid, que proveerá a la misma de las ventajas que he ido exponiendo a lo largo del trabajo.

PALABRAS CLAVE:

Blockchain, Criptomoneda, Smart contracts, Token, Descentralización

ABSTRACT

This final project aims to explain, in a simple and accessible way, how blockchain technology works and its application to the world of cryptocurrencies. How they work, what interest can they arouse and why are they so important in today's financial society are some of the questions that will be resolved in this essay.

It is an extensive and technically complex subject that I intend to narrow down by addressing the fundamental and practical aspects that describe the mechanism of both; the use and development of cryptocurrencies, without diving into the complicated ins and outs of how their codes work, since they require advanced knowledge of mathematics, computing and cryptography.

It is developed in two different parts. In the first part, the conceptualization and basic information of the subject are discussed, in addition to some of the most interesting cryptocurrency projects today and their new decentralized applications and Smart contracts. Within the second part, a practical application is made based on the creation of a cryptocurrency - in the simplest way that I have been able to get right - in order to provide its own token to the Faculty of Commerce of Valladolid, which will provide it with the advantages that I have been exposing throughout the project.

KEY WORDS

Blockchain, Cryptocurrency, Smart contracts, Token, Decentralization

Importancia de esta tecnología en la actualidad

La tecnología blockchain posee las características necesarias para una sociedad como la actual que, basada en la comunicación y las nuevas tecnologías, necesita para validad la información de, como veremos en este proyecto, no solo pagos y transacciones económicas, sino además de un sinfín de posibles usos relacionados con la automatización y certificación de datos que en muchos casos forman parte del ya conocido y también creciente “internet de las cosas”.

Por tanto, ya no es solo las funciones y el desarrollo que ya han tenido lugar y nos aportan las interesantes funciones de las que disponemos en la actualidad,

si no de la perspectiva de futuro que nos presentan y los nuevos caminos a las innovaciones que están por venir, que sin lugar a duda se aprovecharan de esta valiosa herramienta para conformar su funcionamiento.

Intención del trabajo e interés personal para esta investigación.

¿Por qué este proyecto?

Desde que descubrí este mundo de las criptomonedas, me he sentido atraído, casi hipnotizado por todo el ecosistema que se ha formado paralelo a ellas. Tardé unos meses en decidirme finalmente a hacer mi primera compra en un Exchange; en la que recuerdo gastar una parte notable del dinero que tanto me había costado ganar en mi anterior trabajo, incluso recuerdo que las expectativas de este mercado fueron tan positivas que hasta logré convencer a mi padre -bastante escéptico con estos temas- de que invirtiera una pequeña cantidad que no le importara perder en estas "monedas digitales". De esta manera, gracias a esa inversión decidí formarme con más atención en el mundo de las criptos, lo que poco a poco despertó en mi un mayor interés en la tecnología que las sustentaba. En un primer momento he de reconocer que mis premisas y estudio de mercado era bastante deficiente ya que casi toda la información de la que disponía era de fuentes de dudosa calidad y escasa información.

En un momento dado vislumbré la oportunidad de profundizar en este tema mediante la realización de mi Trabajo Final y aquí me encuentro redactando este documento pues no dudé, ni un segundo, en que era el tema apropiado para mí. Aún, a día de hoy, asimilando el conocido reciente desplome de este mercado, mi confianza en las criptomonedas y en su valor futuro mantienen mis perspectivas favorables y positivas hacia ellas. Pero mi interés por estas divisas ha alcanzado un punto más allá de lo meramente especulativo, y es en mi atracción por su funcionamiento donde reside la intención de este proyecto. Como estudiante del Grado en Comercio de la Facultad de Comercio de Valladolid, me veo casi en deuda de realizar mi pequeña aportación a la facultad intentando desarrollar un proyecto de propuesta de creación de una criptomoneda asociada a la facultad.

Agradecimientos

Es de bien nacidos ser agradecidos. Así me gustaría recordar y agradecer a todas las personas que me han ayudado, poco o mucho, en que pueda estar hoy aquí defendiendo mi Trabajo Final con el que espero graduarme en esta Facultad de Comercio de Valladolid que me ha dado la oportunidad de formarme creciendo intelectual y personalmente.

Mi primer y más sentido agradecimiento es para mi familia que ha estado ahí en todo momento, y sobre todo en los más difíciles. Os quiero.

Y por supuesto, a mi tutor Francisco Javier Galán Simón, que me ha apoyado en todo lo que he necesitado y ha tenido una paciencia infinita con la premura del tiempo de presentación. Igualmente hago extensible mi agradecimiento a todos los profesores y personal no docente que me han aportado los conocimientos y competencias necesarias para el desarrollo en este trabajo. Gracias a todos.

Las criptomonedas y la red blockchain. Sus proyectos.

1.1 Contexto

Habiéndose convertido en un tema de actualidad y, en mayor o menor medida, teniendo la sociedad una breve noción de a qué nos referimos cuando hablamos de criptomonedas, e incluso sobre la tecnología a partir de la cual se conforman, considero necesario desarrollar la idea y el concepto sobre el cual se ha basado este trabajo. Este tema al ser complejo y extenso permite su explicación desde distintos enfoques y disciplinas académicas, pero desde mi perspectiva desarrollaré una orientación eminentemente de uso práctico y funcional. Por este motivo, voy a explicar a continuación una serie de conceptos que considero imprescindibles para el desarrollo de este proyecto.

1.2 ¿Qué son las Criptomonedas?

En primer lugar, las denominadas Criptomonedas, son activos digitales que emplean la criptografía para asegurar, validar y certificar sus transacciones, haciendo de éstas un medio de pago seguro, rápido y que además no requiere de ninguna clase de institución o banco central para su regulación, esto significa por un lado que no necesitan que ninguna entidad respalde estas criptodivisas, como por ejemplo en el caso de otras monedas comunes como el Euro o el Dólar, que están avaladas por diversas instituciones como los bancos centrales o los gobiernos de los países que las utilizan y que al mismo tiempo se encargan de su control, emisión, gestión etc... Y, por otra parte, que no responden a los intereses de ninguna jefatura o institución financiera en concreto, y su valor es determinado por el propio mercado. Esto último es uno de los puntos fundamentales sobre el valor de las criptomonedas, estas se encuentran desvinculadas de la economía de una manera directa, por lo que serán independientes en gran medida de la situación económica de cada país y su valor será determinado por la ley de la oferta y la demanda.

Dado que estas monedas existen únicamente de manera digital mediante claves encriptadas, su operatividad se basa en transacciones instantáneas e internacionales a través de internet. En su mayor parte esto se realiza a través del conocido como "*Peer-to-Peer*" (P2P) o red de pares o de iguales, en la cual todos los nodos o puntos que la componen se encuentran a un mismo nivel y pueden interconectarse entre sí de manera indistinta y trabajando conjuntamente bajo el mismo programa o protocolo de funcionamiento.

Ilustración 1 Representación física de criptomonedas

Fuente: newtral.com

Pese a haber sido bombardeados en muchas ocasiones con imágenes de criptomonedas representadas físicamente como monedas reales con una forma y unos materiales concretos, esto se hace únicamente de manera simbólica, ya que son productos intangibles basados en códigos virtuales sin una silueta definida.

Cada uno de los movimientos realizados en esta red se producen directamente desde la cartera de un individuo a la de otro, en la mayoría de los casos actuando a través de un intermediario conocido como: *Exchange*.

1.2.1 Los Exchanges

Existen muchos tipos diferentes de Exchanges disponibles en internet. Estos cumplen principalmente la función que haría un bróker en el mercado de acciones convencional, permitiendo la compraventa o intercambio de criptomonedas entre varios usuarios. Cada Exchange aportará unos beneficios y cualidades específicos sobre los demás como pueden ser el acceso a diferentes monedas y Tokens determinados, ofrecer otras oportunidades de inversión como el "*Staking*" que veremos más adelante o aportarnos datos e indicadores sobre la fluctuación del precio de la moneda en el tiempo: sus valores de capitalización, gráficos sobre su demanda, opciones de trading especiales y una multitud de datos que ayuden al usuario a tomar la decisión de inversión.

Ilustración 2 Función de un exchange

Fuente: bitcoinhardwarewallet.com

Los Exchanges también son medio a través del cual podemos convertir dinero Fiat en criptomonedas de manera directa, estos a su vez cumplen la función de una especie de "monedero" virtual en el que podremos -si lo deseamos- guardar nuestras criptomonedas en nuestra propia cuenta del Exchange, pero a continuación veremos que existen otros métodos específicos destinados a este fin.

Por todos estos servicios, cada plataforma de Exchange generalmente cobra una comisión, esta variara en función del servicio que solicitemos y del programa de intercambio que estemos utilizando.

1.2.1.1 Los Exchanges descentralizados

Dentro de los numerosos Exchanges disponibles, encontramos los descentralizados también llamados DEX (*Decentralized Exchange*), cuya principal particularidad es que no se encuentran sustentados por ninguna entidad central, estos al igual que las criptomonedas se regulan de manera autónoma gracias a su configuración propia basada en *Smart contracts* que aseguran la automatización de todas las tareas que requieran los usuarios para el intercambio de criptodivisas.

Los principales beneficios que nos aportan este tipo de exchanges son la privacidad y anonimato que ofrecen además de su férrea seguridad y velocidad de trabajo, gracias al sistema descentralizado en el que operan que además es completamente transparente para los usuarios ya que suelen trabajar en plataformas de código abierto.

A lo largo de los años, han existido diferentes generaciones de DEX a través de las cuales se han ido implementando mejoras y avances tecnológicos a través de implementaciones como los *Smart contracts* o notables mejoras en su seguridad.

Estos exchanges se desarrollan sobre plataformas de Blockchain como Ethereum, Stellar, Komodo o Neo, que permiten crear sobre ellas aplicaciones descentralizadas (DApps) que explicaré en profundidad más adelante.

1.2.1.2 Otras funciones y utilidades de los Exchanges

De similar manera a como ha ocurrido en el mercado financiero, el mercado de las criptomonedas ha evolucionado mucho debido a su elevado grado de actividad y a la continua aparición de nuevos activos y formas de inversión.

Existen academias de formación en criptoactivos dentro de los exchanges, *pools* de inversión en la que se unen multitud de inversores en un mismo producto buscando sacar rentabilidades pasivas, compra venta de futuros aplicados a criptomonedas, apalancamiento de tokens, *pools* de "*staking*" (que comentaremos más adelante), *pools* de liquidez... y un sinfín de nuevas herramientas y posibilidades, creadas para satisfacer las necesidades de este extenso mercado que en la actualidad abarca cerca de 100.000 millones de dólares.

1.2.2 Como almacenar nuestras criptomonedas: Las *Wallets*

Pese a que el almacenamiento de nuestros activos en el propio Exchange es la forma más sencilla y que más rápido nos permite operar posteriormente con éstos, es también la manera en que más expuestos quedamos a cualquier tipo de hackeo, caída de la plataforma o perdida de nuestros activos; por este motivo la manera más recomendable de mantener nuestras criptomonedas a salvo es mediante del uso de un *wallet* o monedero virtual, cuyo funcionamiento es muy semejante al que podemos encontrar cuando depositamos dinero en un banco: si se lo solicitamos el banco nos abonará la cantidad seleccionada o realizara el pago que ordenemos, y el dinero del que disponemos en la cuenta se encuentra almacenado de manera virtual.

Para el caso de las criptomonedas, debido a que no se trata de un activo físico, en nuestros monederos virtuales se almacenaran las (complejas) claves correspondientes a estos cripto activos, tanto la clave pública, que actúa en función de "número de cuenta", y la cual podremos compartir con otros usuarios, así como la clave privada que representa nuestra "contraseña" personal que permite hacer uso al dueño de las criptomonedas.

Existen varios tipos de *wallets* y cada usuario deberá elegir en función de sus necesidades particulares:

- *Full wallets:* Son las más complejas de todas, y se recomiendan solo a usuarios avanzados que conozcan en detalle el funcionamiento de la red, al mismo tiempo también son una de las opciones más seguras para almacenar nuestras criptomonedas. Este tipo de cartera descarga la totalidad de la Blockchain en nuestro dispositivo (en el caso de Bitcoin, ocupa más de 300GB a día de hoy) y son específicas para cada criptomoneda. Una vez almacenadas en nuestro dispositivo lo convierten en un nodo más de la red, con capacidad para verificar transacciones. Al ser un wallet instalado en el ordenador, se recomienda la instalación de las medidas de seguridad oportunas: antivirus, antimalware, firewall... Dentro de las *full wallets*, la más conocida para Bitcoin es *Bitcoin Core*.
- *Cold Wallets:* Estas almacenan nuestras monedas mediante claves almacenadas o bien en hardware externo o bien en papel, pero de manera *offline*, por tanto, son la opción más segura contra ciberataques, pero en contra se lastra un poco la facilidad para operar con ellas, por lo que están pensadas para almacenar las monedas a medio o largo plazo además de que, al ser un soporte físico, existirá la posibilidad de pérdida o deterioro del mismo. Algunos ejemplos de estas serían: *Trezor* (imagen 1) que consiste en un monedero de hardware en formato similar a un USB o a través de la página de *WalletGenerator.com* que genera códigos impresos en papel los cuales contendrán nuestras criptomonedas (imagen 2).

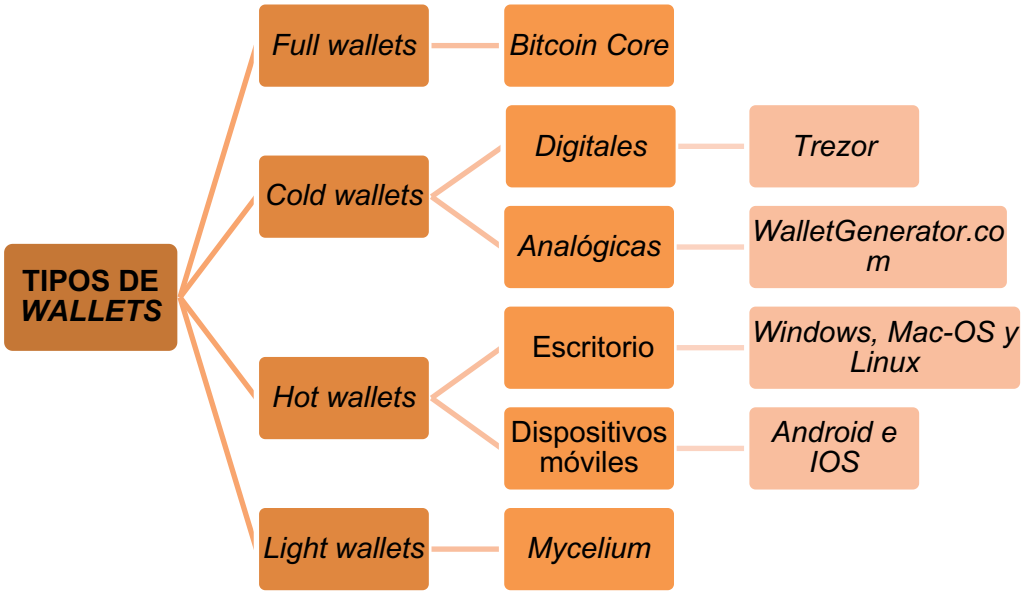
Ilustración 3 Monedero Trezor

Fuente: bitcoin.org.es/Wallets

Ilustración 4 Cartera de: WalletGenerator

Fuente: walletgenerator.es

- *Hot wallets*: Este tipo de monedero virtual permanece constantemente conectado a la red, gracias a su facilidad de uso y rapidez a la hora de realizar operaciones, estas carteras son las más utilizadas por los usuarios de criptomonedas en sus transacciones comunes del día a día. Sin embargo, debido a su exposición continua a internet y aun siendo muy recomendables, su seguridad es notablemente inferior a las opciones vistas anteriormente. Estos programas se instalan como una aplicación o programa en nuestro escritorio, smartphone o tablet o si lo preferimos en muchos casos también es posible en muchos casos el acceso online sin necesidad de instalar nada en el equipo con el que estemos trabajando, a través de estos obtendremos acceso directo a las claves de las criptomonedas que tengamos en nuestro poder. En cualquier caso, es de gran interés para muchos usuarios acceder a ellas a través de un servidor TOR o red de anonimato que nos permitirá aumentar enormemente nuestra privacidad y seguridad a la hora de operar. Una de las *hot wallets* más empleadas hoy en día es *Electrum*, que nos ofrece su versión tanto para escritorio (Windows, Mac-OS y Linux) como para dispositivos móviles (Android e IOS)
- *Light wallets:* este último tipo de carteras en cuanto a su funcionamiento se asemeja bastante a las *full wallets*, solo que en este caso para agilizar su funcionamiento y optimizar sus recursos no se requiere de la descarga completa de la Blockchain, sino solo de una pequeña parte, para su operatividad, se conecta a un nodo que sí tiene descargada toda la red, y desde esa conexión, permite obtener toda la información de la cadena. Son ampliamente utilizadas en dispositivos móviles, como es el caso de *Mycelium* o *Bither*.



1.3 La red Blockchain

Vista una pequeña introducción a los conceptos básicos en el mundo de las criptomonedas, a continuación, veremos los mecanismos correspondientes al funcionamiento de la tecnología que inspira este trabajo.

La Blockchain, en este apartado trataré de hacer una explicación inteligible tratando de evitar los detalles más técnicos y propios de la ingeniería informática que conforman esta red y apuntaré hacia el funcionamiento de la red desde la visión conceptual de su operatividad. Así mismo se hace inevitable hablar paralelamente de la Blockchain y su funcionamiento directo en Bitcoin, por lo que de manera práctica comentaremos la Blockchain y cómo es aplicada en la criptomoneda.

1.3.1 Introducción a la Blockchain

Aquí nos encontramos con la cuestión principal del proyecto, pues es entorno a la red Blockchain que se desarrollan las utilidades de este trabajo.

Para empezar a explicarla crearé un pequeño contexto para entender por qué y cómo nace esta tecnología.

Como sociedad en constante evolución, tras la llegada del internet los seres humanos hemos ido aplicando este medio de interconexión nacido en un primer lugar para

su uso únicamente en ordenadores a trasladarlo casi cualquier cosa u objeto que nos rodea: el conocido como “internet de las cosas” (IoT), que configura cada vez un mundo más digitalizado en el que todo está organizado e interconectado entre sí.

Internet funciona de un modo muy sencillo: un nodo necesita una información de otro, este se conecta al servidor que posee dicha “información” y se la muestra al nodo solicitante; el primero deposita una confianza en que la información que se le ha mostrado proveniente de ese servidor es verídica que es la que hace que esa información posea algún valor, para la mayoría de los casos esto lo consideramos “suficiente” para tomar como válida dicha información, pero al mismo tiempo somos conscientes de lo sencillo que es que estemos siendo engañados y el servidor nos dé un dato incierto o que el servidor al que nos hemos conectado sea falso e incluso que se trate de un simple error, estos son los fallos comunes de la red actual, ya que pese a existir sistemas que aporten un mayor grado de certeza y seguridad, internet plantea numerosos problemas de privacidad y vulnerabilidad a la manipulación de información y, es que por muy robusto que sea el sistema que lo soporte, potente el antivirus que lo proteja o fiable la red que lo gestione siempre existirá la posibilidad de fallo o manipulación.

Por ello cuando necesitamos certificar un dato se necesitará de la presencia una la tercera parte confiable que sea quien otorgue validez entre ambos. Por ejemplo en el caso de una transferencia de dinero la tercera parte confiable sería el propio banco, que es quien aprueba la transacción tras verificar que existen fondos detrás de dicha transferencia y confirmar la identidad de los usuarios, realiza el apunte de entrada y salida en cada una de las respectivas cuentas, generalmente obteniendo una comisión por el servicio, pero no existe en ningún momento un intercambio físico de billetes entre los individuos en el que se envié un “sobre” con el dinero correspondiente. La transacción se efectúa únicamente mediante un apunte contable en cada una de las cuentas.

Fue en octubre de 2008 el momento en el que en un foro sobre la tecnología de la criptografía un usuario bajo el seudónimo de *Satoshi Nakamoto* publicaría un artículo científico explicando una nueva forma de realizar este tipo de transacciones solo que de una manera descentralizada -sin intermediarios-, muy veloz, internacional y completamente infalsificable.

Satoshi estaba perfeccionando una tecnología criptográfica que, si bien es cierto que ya existía con anterioridad, no se había trabajado apenas sobre ella ni se habían creado aplicaciones prácticas reales bajo su protocolo. El post de Satoshi revolucionaría la red informática que conocíamos hasta ese momento, el *Blockchain* desarrollado en su artículo original planteaba la idea de una cadena de bloques encriptados y unidos entre sí

que es capaz de registrar todos los movimientos que se realicen dentro de ella de una manera permanente, inalterable y que además dada su estructura está siendo continuamente vigilada por sus propios usuarios.

Hoy en día no saber quién o quiénes se ocultan bajo el seudónimo de este brillante y misterioso criptógrafo, el "señor" *Nakamoto* a los pocos meses de la publicación de su artículo: *Bitcoin: A Peer-to-Peer Electronic Cash System* puso en marcha su proyecto lanzando el primer bloque de Bitcoin. Esta primera criptomoneda que fue la primera aplicación vinculada a la red Blockchain, se basaba en el desarrollo de un medio de pago globalizado que utilizaba y aprovechaba las ventajas de la cadena de bloques.

Aquí se encontró con el principal problema para la implantación de una nueva moneda en la sociedad: su aceptación, como es lógico aunque la idea detrás de Bitcoin era brillante si la gente no otorgaba el valor necesario a esta criptomoneda jamás podría ser aceptada como medio válido de pago, por este motivo su desconocimiento por parte de la gente y su escasa aceptación como depósito de valor tuvo un comienzo lento y tardo varios años en adquirir el valor y reconocimiento como moneda de cambio.

1.3.2 El funcionamiento de la Blockchain

Para entender el funcionamiento de la gran mayoría de las criptomonedas, se debe comenzar entendiendo el funcionamiento de la red de bloques que la sustenta. La explicación que se hace en este trabajo como ya he comentado es un simple y sencillo esquema ya que la complejidad real de este protocolo necesitaría de mucha más extensión de la que voy a acometer.

La Blockchain es en esencia una cadena de bloques sucesivos que encajan uno tras otro en un orden inalterable y completamente hermético, la información que compone cada bloque es encriptada mediante lo que se conoce como un "*hash*" que en criptografía consiste en un código alfanumérico con una cantidad de caracteres determinada y que se genera a raíz de una compleja fórmula matemática.

El mecanismo es muy semejante al de la encriptación, haciendo que este *hash* sea completamente dependiente de la información contenida en el texto correspondiente al bloque (que en el caso de Bitcoin encontraríamos un registro contable de alrededor de 2.000 transacciones por bloque), si alguien en algún momento intentara modificar, aunque solo sea un dato de la información el código del *Hash* correspondiente cambiaría de manera radical. Como en criptografía, si disponemos de la información original, aplicando la fórmula, es muy fácil obtener el código del *hash,* sin embargo, hacerlo en la dirección

contraria, es decir, a partir del *hash* obtener la información -aun conociendo la fórmula- resultaría prácticamente imposible.

Además de esto, la cadena se asegura de mantener un orden inquebrantable haciendo que cada bloque comience con el *hash* del bloque anterior consiguiendo que estos queden ligados uno tras otro sucesivamente formando una sólida cadena de bloques de información.

Todas estas transacciones se realizan desde direcciones numéricas asociadas a monederos, no a usuarios, por lo que, aunque las transacciones y la cuantía de los monederos son públicos -asegurando una completa transparencia de la red- la identidad de los usuarios o a quién pertenece cada monedero se mantiene de forma anónima.

Pero si almacenáramos esta cadena en unos servidores centrales estos serían altamente susceptibles a ataques, fallos o pérdidas de información. Por tanto para terminar de asegurar tan valiosa información la Blockchain, se vale de los propios usuarios como verificadores de que la cadena permanece inalterada, la Blockchain se almacena en los propios dispositivos pertenecientes a la red, lo que significa que existen millones y millones de copias que se respaldan unas a otras haciendo prácticamente imposible conseguir borrarla de todos y cada uno de los usuarios de la red, y al mismo tiempo si en algún momento esta red tratase de ser alterada, este cambio sería fácilmente detectable por el resto de los usuarios quienes comprobarían el error en el resto de los dispositivos y rápidamente esta "cadena" falsa sería invalidada.

Con todo esto y de manera un poco resumida, la Blockchain sería una base de datos repartida por todos los usuarios de ésta, con un registro almacenado en bloques consecutivos y delimitados por un "código" que los mantiene cifrados y en orden. Todo esto realizado de una manera descentralizada y manteniendo el anonimato de sus usuarios.

1.3.3 Minería

Por tanto, no hay nadie "concreto" que se lucre por ofrecer este servicio a los usuarios, aunque ciertamente si es necesario que existan ciertos nodos que verifiquen todas estas transacciones y se encarguen de generar bloques y asociarlos a su correspondiente *hash*, estos son los mineros.

Los mineros son aquellos usuarios de la red blockchain que se encargan de validar y recopilar todos los datos -como veníamos diciendo en este caso particular de Bitcoin:

transacciones-, comprobarlas, crear un *hash* para este bloque y cerrarlo. Pero para poder cerrar con éxito un bloque es necesario añadir otro dígito especial al final de cada bloque.

Nuestro cierre, también llamado *nonce,* tiene una razón de ser muy importante en el correcto funcionamiento de la red ya que será el encargado de ralentizar el proceso de creación de bloques, y asegurar la propia red frente a ataques informáticos (generalmente de tipo DoS que traten de infectar toda la red de usuarios), su aplicación se basa en algo conocido como “Proof of Work” (PoW) o “Prueba de trabajo”

La prueba de trabajo es el problema matemático que los mineros deben resolver para poder crear un bloque nuevo, este problema requiere un enorme poder computacional para ser resuelto y es adaptativo a la potencia de trabajo total de la red, haciendo que estadísticamente se tarde un tiempo similar en poder resolverlo, de modo que, si el hardware o número de mineros aumenta, también lo hará la dificultad de esta prueba.

Para el caso de Bitcoin, la prueba consiste en obligar a que el *Hash* de todos los bloques comience por un número determinado de ceros. Por ejemplo: “0000000000x8df8s8jjnvw777d80906…”. Para que este comience por el número adecuado de ceros, se deben probar al azar millones de combinaciones en el número de cierre al final del bloque hasta finalmente dar con el acertado. Este proceso tarda cerca de unos 10 minutos que es, por tanto, el tiempo que, como máximo, tardaremos en realizar una transacción.

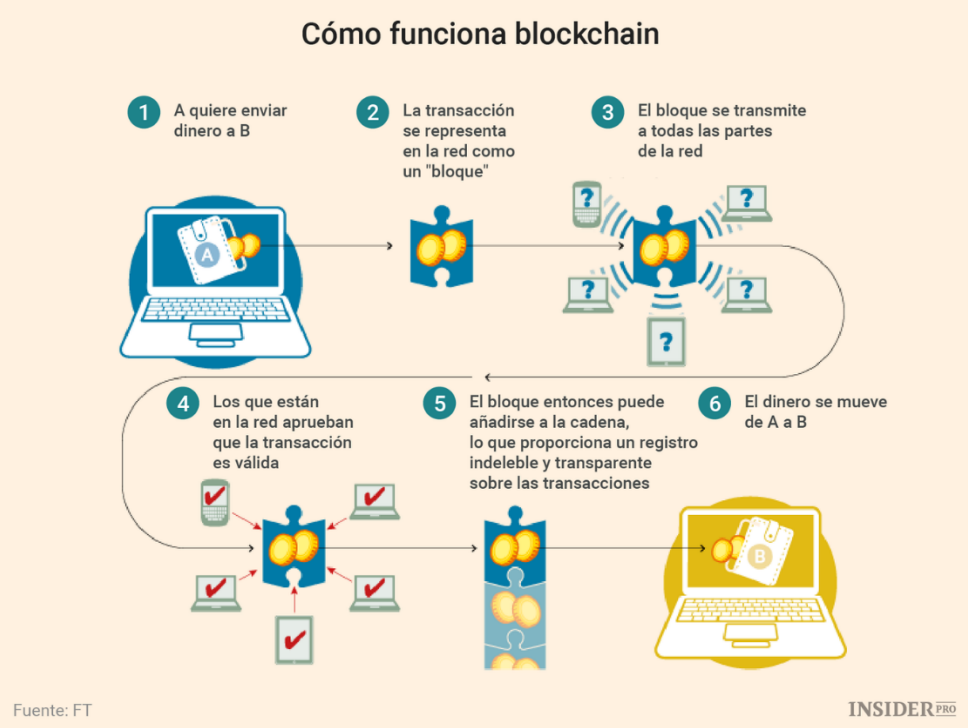
Una vez el minero ha conseguido encontrar este número, enviará el bloque con la solución al resto de usuarios de la red, los cuales deberán comprobar que la información dentro del bloque es correcta y si la mayoría de los usuarios la dan por válida el bloque es añadido a la cadena y se validan todas las transacciones contenidas en él. Hecho esto, cuando el minero añade un bloque a la cadena, obtiene una recompensa determinada por su esfuerzo, de esta forma, además de prevenir ataques informáticos, se consigue que sea más interesante contribuir a que la red funcione de un modo adecuado que intentar hacer trampa o hackearla debido a que merece más la pena intentar resolver y cerrar un bloque para obtener la recompensa que emplear los recursos informáticos para intentar falsear transacciones las cuales además quedarían rápidamente inutilizadas al ser detectadas por el resto de usuarios.

Con todo esto, cada bloque tendría más o menos la siguiente forma:

1) Hash del anterior bloque

2) Registro de transacciones: aprox. 1 Mb, para Bitcoin, unas 2.000 aproximadamente. En este registro se incluyen los números del monedero de cada usuario y la cantidad de fondos que se transfieren.
3) El número de la prueba de trabajo o *nonce* que consiga que el *hash* comience por un determinado número de ceros.

Ilustración 5 Como funciona Blockchain



Fuente: www.blog.wearedrew.com

1.3.3.1 Pools de minería

Con la creciente dificultad en la resolución de los problemas de *hasheado* para el cierre de bloques de la red Blockchain, la mayor parte de los mineros, han decidido agruparse en colectivos llamados: *pools*, en los que comparten recursos informáticos para lograr la obtención de la respuesta acertada y así repartir la recompensa obtenida de forma equitativa entre sus participantes.

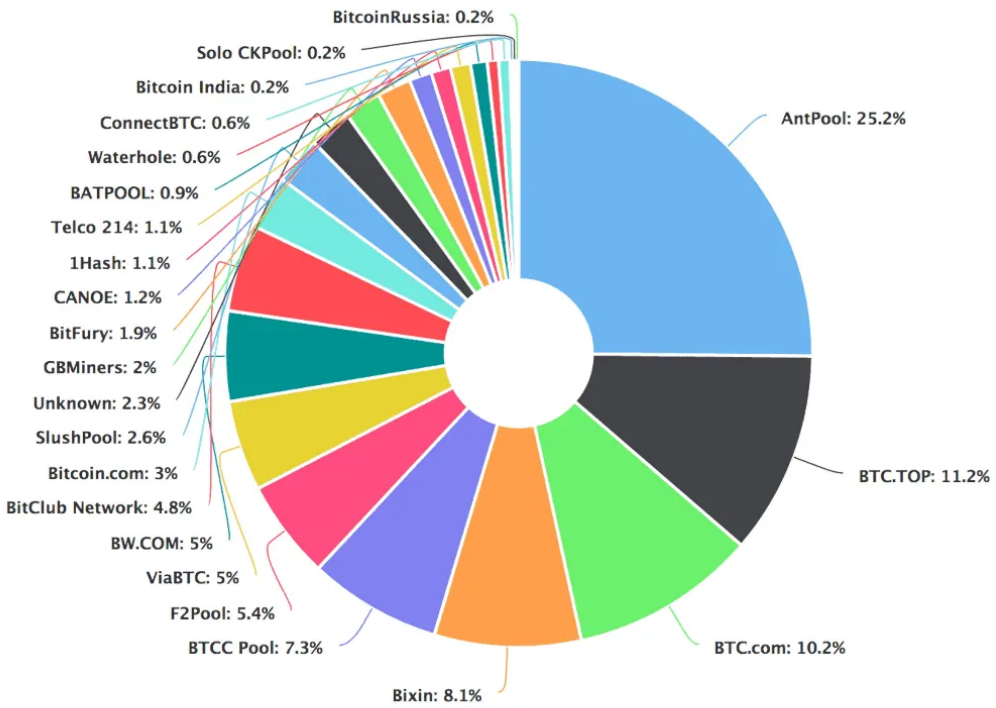
Este trabajo cooperativo de minado es posible gracias a que el protocolo de la mayoría de las criptomonedas que utilizan *Proof of Work* permiten este tipo de minado colaborativo en su código, en el, los mineros trabajan comunicados en un mismo bloque

generando cada uno posibles soluciones diferentes y de forma que no sean repetidas por otros mineros del mismo *pool*.

La posibilidad de minado cooperativo hace posible el minado a los usuarios pequeños que disponen de poca potencia computacional, y que si no fuera por su adhesión a un *pool* de minado no podrían obtener ningún rendimiento.

En la actualidad, estos son los principales pools de minado a nivel mundial:

Ilustración 6 Principales Pools de minería



Fuente: academy.bit2me.com

1.3.3.2 La minería en la actualidad

En la actualidad, la minería ha cambiado significativamente si lo comparamos con sus inicios, inicialmente se minaban bloques enteros con equipos sencillos y la potencia obtenida de un CPU convencional generando unos costes energéticos despreciables, tras el exponencial crecimiento de esta tecnología y la inclusión de cada vez más mineros a red, el coste computacional se ha multiplicado hasta el punto de que lo que antes se podía

minar con un ordenador convencional en casa ahora se realiza en grandes servidores que conectan cientos de equipos consecutivos con tarjetas gráficas de última generación y en grandes granjas de minado situadas en lugares estratégicamente seleccionados para esta práctica como son países con bajo coste tanto eléctrico como de hardware así como zonas muy frías que faciliten la refrigeración de estas potentes instalaciones.

Es por esto por lo que el minado de criptomonedas se ha convertido mayormente en una actividad destinada a mineros "especializados" que pueden permitirse costear las instalaciones y equipo necesarios para esta práctica, ya que con la competencia y las recompensas actuales solo será rentable para los usuarios que optimicen al máximo su ejercicio.

1.3.4 Transacciones válidas

Como último proceso de seguridad, todas las transacciones previamente a poder ser incorporadas a la red Blockchain deben ser validadas para certificar que realmente han sido enviadas de la cuenta del usuario que desea transferir los fondos a la cuenta del usuario que los recibe.

Dicha validación, se produce gracias al mecanismo de encriptación asimétrica, este mecanismo ampliamente empleado en la informática y la banca actual ha sido el método también empleado para garantizar la veracidad de las transacciones. El sistema funciona a partir de dos claves, una pública y otra privada que están ligadas la una a la otra, a partir de la clave pública podemos verificar que una información -la intención de realizar cierta transacción- proviene de forma garantizada de una persona que es la que posea la clave privada. De este modo están aseguradas tanto que las transacciones son reales, como que estas no han sido modificadas en ningún momento.

1.3.5 El Trilema de la escalabilidad de Vitalik Buterin

Pese a las numerosas utilidades del uso de la red Blockchain y sus capacidades excepcionales, existen problemas poco despreciables dentro de esta red, y esto se debe a que no pueden ser resueltos, o al menos en este momento, todos los requisitos deseables de una plataforma "perfecta", y siempre se debe sacrificar algo para poder disponer de una ventaja y en este caso no es una excepción.

Vitalik Buterin (fundador de Ethereum), describe este problema como: "El Trilema de la escalabilidad" ya que en la Blockchain nos encontramos con tres grandes propiedades que posee la tecnología de Blockchain:

- La escalabilidad: Número total de transacciones por unidad de tiempo que el sistema es capaz de procesar (unas 3,5 para bitcoin).
- La descentralización: Nivel de dispersión que mantiene la red entre sus nodos y hace que cuanto más descentralizada esté, más difícil será que sea controlada bajo los intereses de una entidad además de defenderse contra fallos en servidores únicos.
- La seguridad: La red Blockchain basada en *Proof to Work* plantea una controversia en cuanto a su seguridad inquebrantable, existe un tipo de ataque teórico conocido como el "51%" que podría tener consecuencias fatales para cualquier criptomoneda que use este tipo de sistema de seguridad basado potencia computacional, ya que si de alguna forma una entidad lograra hacerse con un poder computacional igual o mayor que el 51% (haciendo que esta deje de ser una red descentralizada) del poder total de la red --el poder de sus mineros-, asumirá el control de la plataforma y esta dejaría de ser completamente segura quedando bajo el control de esta entidad ya que este podría minar mucho más rápido que el resto de los mineros de la red haciendo que el resto de los mineros pierdan interés a al no recibir ninguna recompensa por su minado o la entidad atacante tendrá la capacidad de auto aceptar sus propios bloques fraudulentos.

Según Vitalik no podemos asegurar las tres propiedades al mismo tiempo y por tanto debemos elegir cuál de ellas sacrificar, si decidimos sacrificar la escalabilidad se comprometerá la amplitud de la red haciendo que el sistema no pueda ser ampliamente aceptado como vehículo para realizar transacciones ya que el número de las mismas que se podrán realizar por segundo será escaso en relación a la demanda de las mismas, formándose un cuello de botella que limitaría mucho la operabilidad, sin embargo nos encontraríamos con una red muy segura y con un nivel de descentralización muy elevado.

Por otra parte, si al contrario en lugar de la escalabilidad, fuera el nivel de descentralización el que decidimos rebajar, encontraríamos mayor exposición al control, censura e influencia por parte de distintas entidades que la componen además de aumentar las posibilidades de encontrar puntos de fallo únicos, pero en un entorno en el que se confíe en los nodos de validación como puede ser el empresarial, esta podría ser una opción aconsejable. El comprometer la seguridad es una opción nada recomendable en prácticamente ningún caso puesto que es la principal ventaja de esta red.

Es por esto por lo que diferentes desarrolladores trabajan en las variadas opciones de criptomonedas y proyectos que se adecuan a los distintos escenarios y distintos requerimientos técnicos que se exponen en el apartado referente a las criptomonedas más importantes.

1.3.6 Prueba de Participación

Con motivo del incesante aumento de uso de criptoactivos y por consiguiente de la cantidad de transacciones que se realizan por minuto, la escalabilidad ha tomado un papel muy importante entre las características principales de las criptomonedas, dado el actual volumen de transacciones que requieren de ser validadas para poder acoplarlas a la cadena de bloques esta ha tenido que evolucionar adaptándose a la demanda actual, gracias a esto nació la "Prueba de participación" o *Proof of Stake* (PoS), un nuevo sistema de consenso en sustitución de la anterior *Proof of work.*

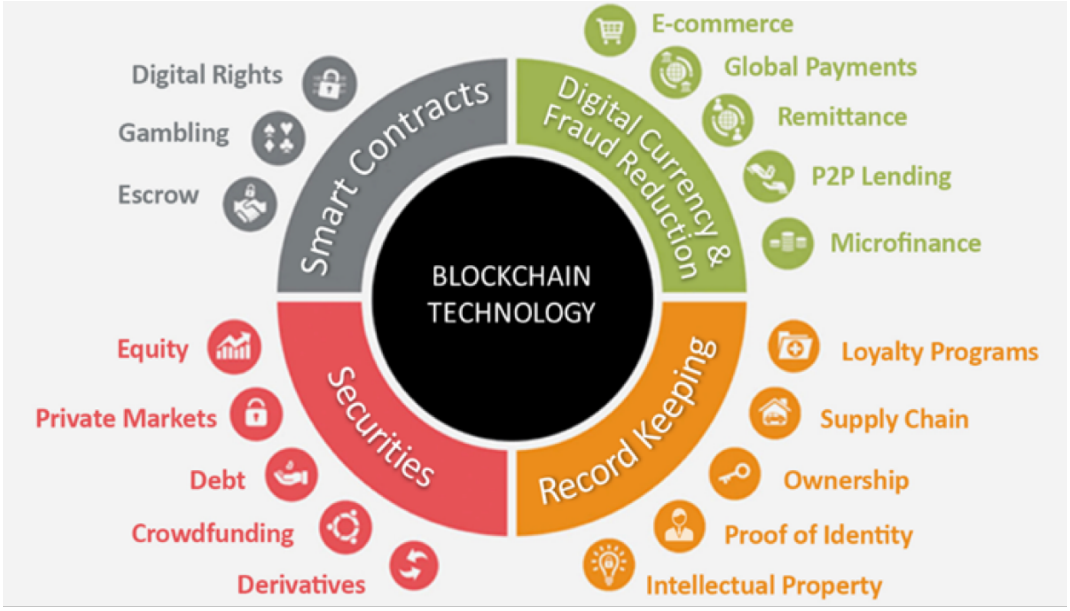
En este sistema, el validador es elegido de entre todos los nodos validadores disponibles en la cadena, puede ser de forma completamente aleatoria o ,como es más común, siendo más probable la asignación a miembros que reúnan una serie de requisitos como pueden ser la antigüedad, el volumen de participación o la implicación en la red, de esta manera se facilita un método que consume muchos menos recursos tanto informáticos como energéticos y al mismo tiempo se mejora notablemente la rapidez a la hora de gestionar transacciones, al mismo tiempo, se aumenta la descentralización ya que mediante la PoW los mineros tendían a agruparse en colectivos muy numerosos, de este modo quedan más diversificadas las funciones de los usuarios y finalmente, la PoS, reduce la supuesta posibilidad de que la red sufra un ataque de 51% ya que en este caso los atacantes no tienen que poseer poder computacional, si no el 51% de las monedas en circulación de esa red, y si un usuario es poseedor de ese porcentaje de monedas en la mayoría de los casos el valor de estas bajara notablemente, por lo que disuade a los posibles atacantes.

El funcionamiento de este sistema se efectúa de la siguiente manera, tomando para el ejemplo que el criterio de elección sea el volumen total de monedas: Cada usuario de la red posee un porcentaje de activos mayor o menor que el de los demás (en función de su inversión), los usuarios que deseen participar en el *Proof of stake* deberán inmovilizar sus fondos para poder validar transacciones dentro de la propia cadena usándolos así como "garantía", en función de estos porcentajes se asignan unas probabilidades y se eligen unos nodos que serán los encargados de realizar estas tareas por las cuales obtendrán una recompensa, pese a aumentar las probabilidades teniendo una mayor reserva, cualquiera puede salir elegido por lo que se asegura la descentralización.

1.3.7 Utilidades de la red Blockchain

La principal y más conocida aplicación de la red blockchain es claramente la de soporte principal para la creación de criptomonedas destinadas a la gestión de medios de pago, sin embargo, no deberían desperdiciarse las interesantes cualidades que nos puede aportar esta tecnología en otros campos.

Ilustración 7 Utilidades del Blockchain



Fuente: acidworldwide.com

Fuera del entorno financiero, esta cadena de bloques puede ser empleada de diferentes ámbitos, vamos a comentar brevemente algunos de ellos:

Forma 1. Como un servicio de almacenamiento en la nube descentralizado, ofreciendo así una capa de protección especial frente a ataques informáticos, o pérdidas de información repentinas al quedar varias copias almacenadas en los distintos nodos de la red, además permitirá disponer de una trazabilidad exacta del archivo y todos sus movimientos. Esto permite a usuarios con mucho espacio de almacenamiento libre rentabilizar ese espacio alquilándolo a compañías que ofrezcan este tipo de servicios, o bien puede utilizarse como recurso interno para empresas en la que la información sea custodiada y compartida por todos los miembros de un equipo de trabajo.

Forma 2. Gracias a las posibilidades de certificación que nos aporta este sistema, nos permitirá también gestionar nuestros usuarios y registros online y no solo podremos identificarnos de manera segura, sino que también podremos ser identificados a través de otros usuarios que podrán garantizar nuestra identidad.

Forma 3. Del mismo modo que la Blockchain de una criptomoneda almacena un registro de transacciones fiable e inalterable, esta, puede almacenar cualquier otra información que queramos anotar en ella, otorgando un grado de seguridad muy superior que cualquier base de datos a cargo de un servidor de terceros, lo que puede ser muy útil en diferentes casos:

- Para el almacenaje de registros médicos en el que quede almacenado todo el historial del paciente eliminando por completo los traslados de información y otros inconvenientes del sistema tradicional y quedando ligado a la persona todos sus antecedentes clínicos.
- Para la asignación y registro de bienes y propiedades a los usuarios, que garantice de forma inequívoca la titularidad de cualquier bien y los vincule digitalmente a una persona o entidad.
- Para el registro de la propiedad intelectual, patentes, derechos de autor y otras licencias intangibles, gracias a este sistema todos los usuarios que lo necesiten podrán disponer de esta información.
- Para llevar un registro de los habitantes de un país (nacimientos, muertes, matrimonios etc.). Todo quedará anotado de manera ordenada y permitirá un control directo de estos datos reduciendo la burocracia.
- Para empresas, facilitará llevar un control de cada cliente y sus interacciones, así como un seguimiento detallado del estado del pedido.

Forma 4. Una de las aplicaciones más notorias que encontramos es la posibilidad de implementar “Smart Contracts” o “Contratos inteligentes” en su código, que son aplicaciones de software autoejecutables bajo ciertas condiciones y que generan un contrato vinculante, pero este es un apartado de interés que desarrollaremos en detalle más adelante.

Forma 5. La Blockchain también permitiría almacenar un seguimiento en las piezas de una cadena de suministros o garantizar el origen de cualquier material. Esto sería fundamental para el comercio sostenible asegurando la legitima

procedencia de los productos además de repercutir beneficiosamente también en el mercado de los productos de lujo (como sello de garantía) o en el mercado del arte verificando su autenticidad.

Forma 6. Blockchain hace un seguimiento actualizado de cualquier documento y al permitirle crear un registro inalterable también asegura la autenticidad del mismo por tanto resulta idóneo como mecanismo "notarial" eliminando al intermediario y reduciendo enormemente los costes derivados de este servicio de certificación de documentos. Además, mejora la seguridad y privacidad respecto a un servicio de notaría convencional.

Forma 7. En el apartado de elementos de seguridad también podemos encontrar interesantes aplicaciones para la interacción con aparatos electrónicos tales como cerraduras, puertas y otros sistemas los cuales al implementarse con la Blockchain puedan automatizar los accesos en función de la persona o los permisos concedidos, eliminando operadores humanos con lo que mejora la seguridad y optimiza costes.

Forma 8. Permite una gestión más eficaz de los contratos de alquiler, en los que por medio de un contrato autoejecutable grabado en la cadena un usuario realizaría la contratación automatizada de (por ejemplo) una propiedad recibiendo acceso instantáneamente en el momento en que el pago es autorizado, esto sería extensamente aplicable para un sinfín de servicios que existen en la actualidad y como en los anteriores casos agilizaría y abarataría el proceso.

Forma 9. La votación a distancia a través de esta tecnología mejoraría las posibilidades actuales de este servicio permitiendo a los usuarios votar de un modo más cómodo y seguro que el actual, además se resolvería uno de los principales inconvenientes del voto remoto actual: el anonimato, que de esta manera quedaría completamente resuelto. Este sistema no solo podría ser empleado para votaciones electorales, si no que para cualquier asunto que deba ser sometido a votación ya sea dentro de compañías, agrupaciones, etc., que podría ser resuelto rápidamente mediante el empleo de un sistema basado en Blockchain.

Forma 10. Se podrían crear redes de micro transacciones que permitirían realizar pagos a compañías por sus servicios de un modo mucho más detallado en función de los servicios que desean ser contratados, algo que en el ecosistema actual generaría un sobrecoste importante al necesitar realizar

muchas más transacciones, pero de menor cuantía. Los usuarios ya no tendrán que pagar por los elementos o el tiempo que no deseen utilizarlos.

Forma 11. La unificación del *Internet of Things* (IoT) con la Blockchain, a partir de 2008, el número de dispositivos conectados a internet superó el número de personas en la tierra, a partir de este momento se habla del nacimiento del IoT. El IoT consiste en las interconexiones y el funcionamiento conjunto de diferente dispositivos, sensores y elementos electrónicos que se comunican y conectan con otros ordenadores dentro de la red de internet, permitiendo su control conjunto y cooperación. La utilización conjunta de la Blockchain con estos sistemas informatizados generará redes auto sustentadas y descentralizadas que compartan información y estén en constante actualización, del mismo modo una gran parte de los sistemas de IoT funcionaran mediante transacciones realizadas por medio de criptomonedas lo que organizará un nuevo orden de pagos automatizados y basados en Smart contracts de una manera completamente despersonalizada ya que tanto los emisores como los receptores de estos pagos podrán ser maquinas programadas. Uno de los principales proyectos trabajando en la unificación de estas dos tecnologías es IOTA (Internet of Things Application)

Estas son solo algunas de las aplicaciones posibles del amplio abanico que nos brinda este concepto: aplicaciones militares, nuevos tipos de servidores, medios de comunicación... En este momento existen numerosos proyectos que buscan dar un nuevo servicio o mejorar uno ya existente mediante la aplicación de este protocolo que nos permitirá transformar por completo el actual modo de vida y seguirá con la línea de tendencia actual hacia la automatización de todos los procesos posibles.

1.4 ¿Qué valor nos aportan las criptomonedas?

Durante la última década, las criptomonedas se han abierto un importante hueco dentro de la economía mundial, su utilización se resume como un nuevo medio de pago que mucha gente considera más bien un instrumento especulativo, pero como ya hemos mencionado, el valor que estas nos han conseguido aportar es mucho mayor del que a priori pueda parecer. Detrás de casi todas las criptomonedas existe un proyecto y una finalidad específica que trata de ofrecer un nuevo servicio o resolver un problema actual aprovechando las ventajas que nos brinda la Blockchain, dicho de otro modo, cada una de las monedas se creó y configuró con un objetivo.

Para entenderlo de forma más práctica con un ejemplo tenemos al gran coloso de las criptomonedas: Bitcoin, además de sus valores especulativos, esta criptomoneda nos muestra su principal particularidad que es brindarnos la capacidad de poder realizar transacciones de manera internacional con un mínimo coste y en cuestión de minutos, que en comparación con cualquier otra divisa tradicional se ha conseguido declarar vencedora absoluta.

Con esto quiero transmitir, que cada criptomoneda existente, en mayor o menor medida, nace con una propuesta de valor que es la que la hace especial y diferencia del resto, también forma parte de este concepto el valor especulativo que presentan ya que cuando se lanza una nueva moneda al mercado a través de un *Initial Coin Offering* (ICO) es gracias a este valor especulativo determinado por el interés que suscitan las características particulares del proyecto, será el motivo por el que los inversores apuesten por estos proyectos y los financien mediante la compra de sus activos.

Además, otra de las principales aplicaciones que nos brindan consiste en la reserva de valor, al igual que el oro las criptomonedas de uso público, son susceptibles de emplearse como reserva de valor ya que su valor inicialmente se espera que se mantenga o aumente con el paso del tiempo esto se debe a que en primer lugar su creación se encuentra limitada en muchos casos con topes de emisión (totales o temporales) por tanto además de limitar su salida al mercado eliminando problemas los posibles problemas de inflación que suelen contraer el resto de divisas, garantiza que su valor no se devaluara, esto sumado a que no responden ante ninguna entidad, estado o individuo gracias a su descentralización poseen una independencia total también las aleja de la posible manipulación o intervención estatal.

Además, son bienes extremadamente accesibles a nivel global, que funcionan indistintamente en cualquier país por lo que funcionan como una excelente herramienta del comercio internacional.

Es por estos motivos, sumados a la trayectoria que han tenido en el mercado a través de la última década por lo que las criptomonedas han conseguido consolidar su posición en el mercado y demostrar su funcionalidad real.

1.4.1 Diferenciación entre Token y Criptomoneda

Cuando hablamos de criptomonedas en general, es importante conocer cuando hablamos de una criptomoneda propiamente dicha y cuando lo hacemos de un Token, la principal diferencia entre ambos reside, en que una criptomoneda posee su propia red

Blockchain característica, mientras que los Tokens se encuentran basados en la Blockchain de una criptomoneda existente, como por ejemplo podrían ser la de Ethereum, Waves, Tron, etc.

Los Tokens son activos digitales empleados como medios de intercambio dentro de una comunidad, que es la que les otorga su valor real. Para entenderlo mejor, podemos entender los Tokens como si fueran las fichas de un casino, estas son emitidas por un casino para su uso exclusivo dentro de ese casino y no tendrán validez en otros casinos, del mismo modo los usuarios de ese casino lo emplearán como medio de intercambio entre si otorgándole una aceptación a su valor nominal por que confían en que el casino respaldará estos activos, muy parecido a como ocurre con el dinero fiduciario.

Si por ejemplo intentáramos comprar una barra de pan empleando estas fichas fuera del casino muy dudosamente serán válidas como medio de pago porque no existe esa aceptación que encontramos dentro del casino. Los tokens digitales funcionan de un modo muy parecido, solo que gracias a la criptografía solucionan varios problemas que encontramos con los tokens físicos como por ejemplo la extensión de su comunidad o la falsificación que gracias a la red Blockchain, todas las transacciones efectuadas con estos tokens, serán seguras y verificables además conseguimos escapar del control organizado de una sola entidad como sería el casino, así mismo el valor concedido o de intercambio de estos Tokens dependerá de su demanda en el mercado, otorgado por los propios usuarios, la cantidad de éstos en circulación, el precio que determine su desarrollador etc…

1.4.1.1 Colored Coins

En un primer lugar y dado que la primera criptomoneda en aparecer fue Bitcoin, los primeros Tokens se crearon también a raíz del código abierto de esta criptodivisa, las conocidas como “Colored Coins” estas utilizaban el mismo código que Bitcoin solo que a este se le asignaban unas características propias especiales que lo diferenciaban de su protocolo original y solo permitían su transacción y almacenamiento mediante nodos y monederos adaptados.

Estos Tokens permitían asociar la innovadora tecnología y ventajas de la red Blockchain a casi cualquier cosa del mundo actual: Tokenizar, asociar Tokens a monedas, bonos, bienes etc. En definitiva, crear redes de transacciones basadas en la tecnología Bitcoin, pero en este caso pudiendo hacer partícipe cualquier activo que se nos ocurra.

Su creador, Meni Rosenfield, publicó a finales de 2012 el “*Whitepaper*” con las ideas principales y el modo de actuación de estos nuevos activos, y fue en 2013 cuando se configuro finalmente el protocolo de las *Colored Coins.* Años después se continuó

desarrollando estos Tokens con nuevos protocolos que simplificaron el camino para la creación de más Coins y que además permitían más diversificaciones del script original.

1.4.1.2 ¿Cómo han evolucionado los Tokens Criptográficos?

La creación de las *Colored Coins* supuso un importante avance para los posteriores proyectos de Tokenización ya que con la llegada de nuevas criptomonedas y sus consiguientes redes de Blockchain nuevos tipos de Tokens basados en otras monedas comenzaron a aparecer, como ya comentamos: Waves, TRON, NEM, Omni, etc… pero fue tras la llegada del proyecto Ethereum cuando se abrió un nuevo mundo de posibilidades y utilidades, el proyecto Ethereum permitía la creación de manera sencilla de Tokens por parte de casi cualquier persona o entidad gracias al recién programado protocolo ERC-20, que presume de gran aceptación global debido a su facilidad de uso y amplia compatibilidad con casi todos los monederos actuales.

1.4.1.3 Tokens NFT

Los tokens NFT o tokens “no fungibles”, son tokens creados con el objetivo de dar una representación digital única, indivisible y que es susceptible de asociarse a objetos (reales o virtuales), con el objetivo de poder hacer una “identificación digital” completamente segura.

A efectos generales, son un modo de representación única e irrepetible de algo, por tanto, sus utilidades abarcan desde la propia identificación personal, actuando como si fueran el “DNI” de alguien, hasta la creación de tokens asociados a obras de arte, tarjetas coleccionables e incluso tweets de personas influyentes pasando por objetos como coches o propiedades que gracias a estos pueden ser indeleblemente asociados a una persona. Casi cualquier cosa es susceptible de convertirse en un token NFT, es por esto por lo que son muchas las formas de hacerlo, pero sin duda la más conocida en la actualidad es a través de Ethereum, y los contratos inteligentes que crean un certificado digital de propiedad.

Entre las principales ventajas que nos ofrecen, se encontrarían su indiscutible autenticidad e indivisibilidad, el enorme abanico de posibilidades de tokenización que nos abren y el sencillo proceso de intercambio y almacenamiento que cada vez se encuentra más extendido.

Por contras encontramos una infinidad de protocolos diferentes y continuas actualizaciones de estos que hacen que siempre haya que prestar atención a la plataforma

sobre la que se desarrolle el token en concreto y además muchas de estas plataformas pueden cobrarnos comisiones por sus operaciones.

2 Proyectos y criptomonedas principales o con mayor interés para nuestro fin

Tras la llegada en 2009 de Bitcoin como primera criptomoneda y como primera aplicación práctica de la red Blockchain, una multitud de proyectos con diferentes aplicaciones han ido paulatinamente incorporándose al mercado de criptomonedas actual. Estos proyectos responden a nuevas utilidades aplicables o mejoras y actualizaciones de proyectos anteriores. En este apartado serán analizadas las principales criptomonedas y los proyectos sobre los que se conforman estos activos, para ello serán divididas en diferentes categorías en función de las funcionalidades que nos ofrezcan.

2.1 Criptomonedas relacionadas con medios de pago

Las monedas que encontraremos en este grupo son susceptibles de ser empleadas como medio de pago o como sustitutivo del dinero fiduciario convencional. Son las que, por lo general, tienen mayor capitalización de mercado y aceptación general.

2.1.1 Bitcoin

Como ya hemos comentado anteriormente, Bitcoin fue la primera criptomoneda en aparecer y la referencia para otras muchas que surgieron a continuación. Bitcoin se fundamenta sobre la red Blockchain y actualmente es el buque insignia de todo el criptomercado, por lo que sus movimientos inciden directamente en las fluctuaciones del resto de criptomonedas.

Ilustración 8 Logotipo de Bitcoin

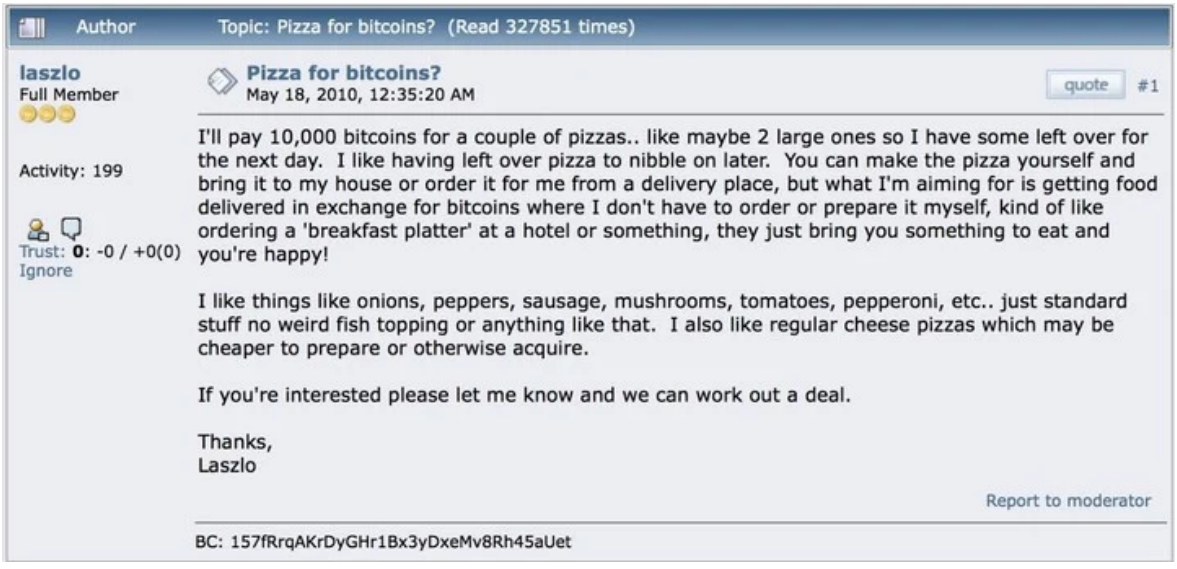
Fuente: shutterstock.com

2.1.1.1 Desarrollo

Tras su apertura al público mediante el artículo del Sr. Satoshi en 2008 y debido a que no existían transacciones previas para conformar el primer bloque de Bitcoin -el conocido como "Bloque *Génesis*"- mediante el algoritmo del *hash*, que dio origen a los primeros 50 Bitcoins de la historia, minados por el propio Satoshi Nakamoto. Hash cuyo contenido fue realizado a partir de una página del periódico la cual se pedía encriptar.

Los posteriores bloques a éste fueron minados por otros usuarios cercanos del foro que consideraron que esta moneda podría tener mucho potencial en el futuro y no se equivocaron. La primera compra documentada que se realizó con esta criptodivisa fue el 22 de mayo de 2010, en la que un programador estadounidense pagó 2 pizzas con 10.000 Bitcoins que en aquel momento tenían el valor de aproximadamente 40$ -en la actualidad esto sería impensable puesto que hablaríamos de alrededor de 400 millones de dólares traducido al valor actual de la moneda-, más allá de la curiosa anécdota nos encontramos con un hito muy importante para la historia de Bitcoin, puesto que por primera vez se le otorgó el valor real como instrumento de cambio que es el mecanismo mediante el que recibe su valor. Anterior a esto su valor se trató de determinar en base al costo energético necesario para minarla, pero esa estimación no era del todo práctica.

Ilustración 9 Mensaje foro Bitcoin



Fuente: Bitcointalk.com

Posteriormente la moneda fue tomando valor paulatinamente debido al aumento de la demanda por parte de los inversores que la encontraban cada vez más interesante como

activo especulativo en vista que en el futuro se consolidase como un medio de pago aceptado y generalizado. Fue durante este año 2010 cuando surgieron varios exchanges pioneros que permitirían aumentar paulatinamente el valor total de Bitcoin alcanzando ese mismo año el primer millón de dólares de capitalización de la moneda. Aquel año el Bitcoin alcanzó un valor de 0,50 dólares en la popular plataforma de trade Mt.Gox, que por aquel entonces acaparaba cerca del 70 % del volumen de intercambios total de Bitcoin. También fue en ese año cuando surgió el primer pool de minería de Bitcoin: *SlushPool* desde el que, por primera vez, una agrupación de mineros comenzó a trabajar juntos en vistas a mejorar su productividad y eficacia.

Fue un año más tarde, en 2011 cuando comenzaron a aparecer, atraídos por el rápido desarrollo de la criptomoneda, los primeros competidores reales de Bitcoin que en sus inicios trataban de ofrecer servicios aumentados de la criptomoneda: mayor velocidad de transacción, anonimato real, etc... Estas monedas fueron Litecoin y Namecoin, cuya programación está basada en el código de Bitcoin. Finalmente, en febrero de este año Bitcoin alcanzó la paridad con el dólar estadounidense (1 BTC = 1 $).

En este punto álgido de proyección de la moneda y su enorme crecimiento, a mediados de ese año la conocida plataforma: Mt. Gox comunicaba a sus clientes que había sufrido un ataque por el cual 850.000 bitcoins habían sido sustraídos de las cuentas de sus usuarios. Posteriormente pudo recuperarse una parte del botín y observándose que el fallo no fue por quebrantar la seguridad de la Blockchain, si no las identificaciones de un trabajador del Exchange. Esto supuso un duro golpe al valor de la criptomoneda ya que se tradujo en una falta de confianza e inseguridad hacia ella.

En noviembre del 2012, tuvo lugar el primer halving de la historia de Bitcoin, tras minarse los primeros 210.000 bloques de la criptomoneda, pasándose de los 50 bitcoins de recompensa iniciales a 25, pero tuvo una repercusión positiva en su valor al aumentar la escasez de esta.

A partir de entonces, la moneda pese a haber experimentado una tendencia (leve) alcista, no ha reflejado hitos de mayor importancia y se ha mantenido trabajando “en la sombra” hasta hace unos pocos años donde tanto ésta como otros proyectos similares han revolucionado el mercado.

2.1.1.2 Bitcoin en la actualidad

En los últimos 4 años es cuando Bitcoin ha experimentado su punto álgido habiendo crecido hasta un 600%, haciendo de esta moneda el criptoactivo fundamental de los

actualmente existentes y marcando su presencia de forma indeleble en la sociedad financiera actual.

En primer lugar, tanto el valor como la capitalización de esta moneda, son los más elevados -de forma notable- de todo el mercado de criptodivisas; su precio, aunque sea uno de los más consolidados y estables está sujeto a fuertes fluctuaciones por distintas variables socio-económicas.

A modo de ejemplo, recientemente ha presentado una fuerte volatilidad oscilando desde su máximo histórico durante el presente 2021 superando los 60.000$ a caer por debajo de los 30.000$ debido a las fuertes correcciones que han tenido lugar por distintos motivos. Así, ha recibido duras correcciones a la baja por la incertidumbre en la aceptación de criptomonedas como medios válidos de pago.

En cualquier caso Bitcoin, tras la pandemia del Covid-19, cobró una importante relevancia entre inversores de todo el mundo al demostrar ser el único activo que adoptó una tendencia positiva durante la crisis sanitaria. Esto le llevó de alcanzar un pico de 63.000$ (aprox. 52.000 Euros) a derrumbarse debido a la fuerte especulación que maneja esta criptomoneda. Esto muestra la enorme “sensibilidad” en su precio a la acción de algunos agentes como por ejemplo el fuerte desplome ocurrido debido a los Tweets de Tesla acerca de que dejaban de aceptar Bitcoin como medio de pago en su web. No solo afectó a la aceptación de Bitcoin como medio de pago válido, si no que supuso que uno de sus principales defensores (El fundador de Tesla, Elon Musk) estaba actuando en contra de los intereses de la criptomoneda y provocando fuertes tensiones que ocasionaron un enorme desplome en cuestión de horas sobre su precio. Algo que desconcertó a los inversores, ya que en el pasado el propio Elon había sido artífice de varias subidas considerables anunciando su fuerte interés por esta moneda.

Este fuerte desplome sufrido en febrero de 2021 fue fuertemente agravado tras unas declaraciones del Banco Central Chino en las que se hablaba de la falta de validez legal e inmadurez del proyecto de las criptomonedas, y sucesivamente el gobierno chino prohibió el minado de criptomonedas en su territorio. A estos ataques se sumaron varias acometidas contra la moneda en la mayoría de los casos alegando que la utilización de criptomonedas es altamente ineficiente en términos energéticos y que su valor queda demasiado determinado por la especulación a la que se exponen.

Tras esta serie de acontecimientos desfavorables para la moneda, en junio de este año presenciamos un importante hito en la implantación de esta moneda en la sociedad: El Salvador se convertirá en el primer país en adoptar Bitcoin como moneda de curso legal,

por tanto, según nos indican fuentes como la BBC: "*Los artículos de un supermercado, por ejemplo, pasarían a poder pagarse tanto en bitcoin como en dólares. El tipo de cambio entre el bitcoin y el dólar será establecido libremente por el mercado"*. También se menciona que todas las deudas u obligaciones determinadas anteriormente en dólares (la moneda actual del país) podrán ser liquidadas en Bitcoin si se prefiere. El presidente del país: Nayib Bukele, niega que la intención con la implantación de Bitcoin sea expulsar el dólar como moneda de curso legal en el país y añade: "*Tratamos de permitir la entrada de emprendedores, talentos e innovadores a nuestro país. No creo que tener el dólar le haga ningún daño. Al contrario, creo que va a ayudar que ambas monedas sean de curso legal*". El Salvador es el primer país que se ha atrevido a dar este paso y pese a ser criticado por muchos y aplaudido por otros de momento habrá que esperar para ver cuáles son los efectos de esta maniobra en el futuro.

2.1.1.3 Características fundamentales.

En cuanto a las características fundamentales de Bitcoin, la principal es probablemente su elevado grado de descentralización la cual le permite ofrecer un elevado nivel de transparencia en sus operaciones sin necesidad de identificar por completo a sus usuarios

Esta moneda como ya hemos comentado recibe su valor en función de su demanda como instrumento de cambio haciendo que su precio sea notablemente volátil en función de la fuerte especulación que se ejerce sobre ella. Sin olvidar que uno de los puntos principales que influyen directamente en su valor es el hecho de que la oferta de Bitcoins en el mercado -a diferencia de las monedas convencionales- en este caso es limitada a 21 millones de unidades, de los cuales algo más 19 millones han sido minados hasta la fecha, cada 10 minutos se añaden 6,25 Bitcoins más a esta cifra en forma de recompensa a los mineros. Esta recompensa se ve menguada notablemente de los 50 bitcoins entregados inicialmente, y es que esta cifra va reduciéndose continuamente debido al conocido como: *Halving* de Bitcoin.

El *Halving* es el acontecimiento en el cual la recompensa entregada a los mineros a cambio de su esfuerzo computacional se reduce a la mitad cada aproximadamente 2.010 bloques minados (Cada 4 años aproximadamente), esto se produce con la intención de poder controlar el tiempo restante hasta el fin de la emisión de monedas y la cantidad de éstas en circulación, esta limitación persigue obtener un modelo en el cual el valor de las monedas aumente con el paso del tiempo (deflacionario), según explica Javier Pastor para Xataka en su artículo: *"Qué es el 'bitcoin halving' y por qué está provocando que el valor*

de bitcoin crezca un 18% en las últimas 24 horas" "El principio básico es similar al del oro: son bienes finitos que cada vez es más difícil obtener" Y esto se debe a que de la misma manera que ocurre con el metal precioso, cada vez es necesaria una mayor cantidad de recursos para obtener una cantidad menor de recompensa bruta, pero el valor generalmente será mayor, como ya ha demostrado en anteriores halving el precio tras reducir la recompensa tiende a aumentar de manera sustanciosa debido a la mayor escasez de estos bienes y al conocido como "miedo a quedarse fuera" y no aprovechar la oportunidad de obtener beneficios.

En la actualidad se encuentran "minados" o sea puestos en manos de los usuarios cerca del 90% de la oferta total de Bitcoins existente y pese a que en 2021 llevamos menos de 12 años desde que el primer bloque fue minado, se espera que el último bitcoin para completar los 21 millones sea liberado en 2140 debido al fraccionamiento progresivo de las recompensas. A pesar de que las recompensas sigan disminuyendo a este ritmo, el valor de cada moneda es cada vez creciente por lo que a medio plazo el valor de recompensas es incluso mayor si se compara con el valor pasado.

Pero, en el momento en que se hayan entregado todas las monedas a los mineros ¿Quién se encargará de validar todas las transacciones de la red para que pueda continuar con su funcionamiento? Satoshi también tuvo esto en cuenta, por lo que en el momento en que no queden recompensas que entregar, los mineros recibirán comisiones por su trabajo, haciendo que no pierdan el interés en los bitcoin y mantengan su actividad en marcha.

El código de esta criptodivisa al igual que su registro de transacciones es público y abierto lo que significa que cualquiera puede comprobarlo, editarlo y mejorar esta red. Así, miles de usuarios de todo el mundo colaboran en las constantes actualizaciones del sistema, haciéndolo más eficaz, seguro, rápido y funcional.

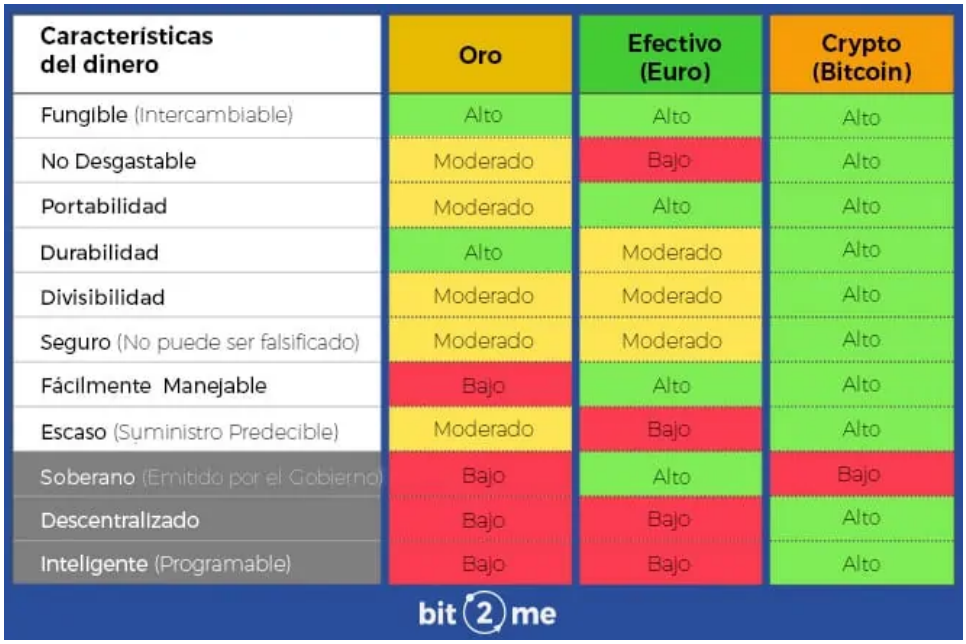
Los principales beneficios directos que nos aporta esta criptomoneda son:

- En primer lugar, la velocidad con la que nos permite trabajar, ya que se pueden mover grandes cantidades de dinero en menos de 10 minutos, además nos permite crear cuentas y monederos de manera muy sencilla y veloz comparado con la lentitud que encontramos en la tramitación a través de entidades bancarias.
- El reducidísimo costo que nos plantea por transacción hace que sea una opción de pago excelente debido a sus bajas e incluso inexistentes comisiones. Esto además abre la puerta a la realización de micro pagos que de otra forma sería insostenible con el sistema actual.

- Es una forma de pago global que no responde a ningún país por lo que puede ser utilizada en cualquier lugar del mundo.
- Es un sistema descentralizado que no queda bajo el control de ninguna entidad o administración por lo que se encuentra totalmente despolitizado y que no es susceptible de utilizarse como herramienta de control para la población o la economía.
- La titularidad de esta divisa corresponde a su portador al 100% y está completamente libre de intervenciones por parte de ningún estado.
- Es fácil su implementación mediante mecanismos de pago automatizados o Smart contracts para que los emisores o receptores de dichas transacciones puedan ser maquinas ejecutando programas.
- La seguridad es uno de los puntos fuertes de este sistema, gracias a la aplicación de uno de los mecanismos criptográficos más avanzados del mundo y la distribución de copias del libro contable entre cientos de miles de nodos alrededor del mundo lo hacen al mismo tiempo resistente a todo tipo de desastres naturales, ataques humanos, fallos...
- Posee un nivel de transparencia máximo en el que todas las operaciones pueden ser comprobadas a tiempo real, por lo que se pueden comprobar todos y cada uno de los gastos hechos por cada cuenta de manera pública.
- Al tratarse de una plataforma de código abierto, cualquiera que lo desee puede libremente editarlo o mejorarlo y si esa mejora es aprobada por votación, será puesta en marcha. Esto provoca que la plataforma este siendo continuamente mejorada por los usuarios y que además pueda adaptarse a las posibles necesidades cambiantes del sistema.
- Todo el funcionamiento de Bitcoin se basa en el consenso grupal de sus usuarios: tanto las mejoras propuestas para su código, como todos los apuntes de registros de transacciones realizadas.
- Bitcoin posee un tope de emisión cerrado en 21.000.000 unidades, esto le asegura inmunidad contra problemas económicos de monedas convencionales como la inflación.
- Pese a no ser un sistema totalmente anónimo, Bitcoin protege la identidad de sus usuarios registrando únicamente el número de monedero involucrado en la transacción, el cual no necesariamente debe estar asociado a tu identidad personal.

Estas son algunas de las ventajas generales que nos propone la red de Bitcoin, pero existen un sinfín de nuevas utilidades, aplicaciones y virtudes del uso de este sistema frente al sistema monetario tradicional.

Ilustración 10 Comparación: Oro, Efectivo y Bitcoin



Características del dinero	Oro	Efectivo (Euro)	Crypto (Bitcoin)
Fungible (Intercambiable)	Alto	Alto	Alto
No Desgastable	Moderado	Bajo	Alto
Portabilidad	Moderado	Alto	Alto
Durabilidad	Alto	Moderado	Alto
Divisibilidad	Moderado	Moderado	Alto
Seguro (No puede ser falsificado)	Moderado	Moderado	Alto
Fácilmente Manejable	Bajo	Alto	Alto
Escaso (Suministro Predecible)	Moderado	Bajo	Alto
Soberano (Emitido por el Gobierno)	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Inteligente (Programable)	Bajo	Bajo	Alto

bit 2 me

Fuente: academy.bit2me.com/ventajas-bitcoin/

2.1.1.4 Ventajas de la utilización de Bitcoin para los comercios.

En cuanto a su aplicación y mejoras en el ámbito empresarial, también encontramos utilidades particularmente beneficiosas para el comercio, como pueden ser:

- La protección contra fraudes debido a que, mediante el pago con bitcoin no se pueden revertir los recibos, haciendo que los comercios puedan evitar estafas y cancelaciones de pagos.
- El coste de las comisiones es nulo o mínimo, además mediante el empleo de Bitcoin no tendremos mínimo de transacción, no como con otras plataformas de transacciones que además de suponer unas comisiones notablemente superiores, en muchos casos nos impondrán un importe mínimo para realizar la transacción.
- Es una forma de pagos que permite a las empresas mantener sus ingresos a salvo sin necesidad de tener grandes equipos de seguridad contratados.

Además, agiliza las labores de recaudación y optimización de tiempo de los empleados al eliminar la necesidad de cuadrar los saldos de caja.

- Los clientes verán la posibilidad de pago en Bitcoin como un avance tecnológico en nuestro comercio y mejorara la percepción que estos tienen de nuestro negocio al ver que se encuentra actualizado con sus medios de pago innovadores.
- No cabe la posibilidad de error humano en la validación de un pago con Bitcoin al ser un proceso automatizado.

2.1.1.5 Principales inconvenientes de esta criptomoneda

Pese a las muchas virtudes de este sistema, existen puntos débiles que en parte son responsables de que aún la aceptación sistemática y global de Bitcoin avance a un ritmo muy lento y disperso. Algunas de estas desventajas son:

- El principal obstáculo con el que nos encontramos, es la exagerada volatilidad de las criptomonedas, no debemos olvidar que -al menos por el momento- nos encontramos con activos sobre los que ejerce una fuerte presión especulativa, y Bitcoin, no es una excepción y pese a ser probablemente es la criptomoneda con mayor consolidación en el mercado, y la mayor parte de esta divisa se encuentra en manos de inversores cuyo único objetivo es obtener una rentabilidad revendiendo la moneda en momentos en los que su valor se dispara. Todo esto, hace que veamos fluctuaciones muy fuertes en poco tiempo y pese que a largo plazo su valor se mantenga al alza resulta arriesgado mantener una cartera para pagos con Bitcoin en el corto plazo.
- Su aceptación pese a mantenerse creciente, sigue siendo minoritaria y no es fácil que acepten Bitcoin en el establecimiento al que acudamos, por lo que sus posibilidades de uso de momento se encuentran limitadas por este motivo.
- El “anonimato” de Bitcoin ha desembocado en la extensión de su uso para la realización de actividades delictivas tales como la compraventa de armas y drogas, este uso en la actualidad no es del todo recomendable debido a que, pese a que en cierta medida el monedero no tiene por qué estar vinculado a una persona concreta, sí que es posible trazar las transacciones realizadas desde este por lo que los delincuentes no se encuentran completamente protegidos en esta red.

- Todo tu dinero se encuentra ligado a tus claves o tu monedero, la férrea seguridad que ofrece Bitcoin se puede volver en tu contra, ya que si por algún motivo perdemos u olvidamos nuestras claves los Bitcoins asociados serán perdidos para siempre y no existirá forma alguna de poder recuperarlos. Se estima que, en la actualidad, alrededor de 4 millones de Bitcoins han sido perdidos para siempre.
- De la misma forma que con la seguridad, el hecho de que no exista alguien que regule la moneda puede tornarse en nuestra contra, ya que reduce enormemente la confianza de algunos particulares y en especial de los bancos, quienes ven esto como una falta de estabilidad importante.
- El límite de emisión fijado para protegerse frente a la depreciación, también puede ocasionar una depresión en la economía por dos motivos, el primero es la incertidumbre generada al minar el último Bitcoin ya que pese a estar establecido un plan por el que los mineros obtendrán una recompensa en forma de comisiones genera una situación de incertidumbre que provocara inestabilidad en la moneda, además de que al existir una cifra finita muchos inversores pueden negarse a poner en circulación sus monedas estancando este sistema económico.

2.1.2 Bitcoin Cash (BTH)

Para la creación de esta criptomoneda, se realizó un *Hard Fork* del código original de Bitcoin, esta renovación persigue como objetivo aumentar la tasa de transacciones por segundo para hacerla más rápida y eficiente a la hora de operar, con vistas a ser susceptible de ser empleada como moneda de intercambio para el día a día.

Ilustración 11 Logotipo de Bitcoin Cash

Fuente: criptopasion.com

En 2017, se renovó el protocolo de Bitcoin, manteniendo todo bajo el mismo código salvo el tamaño de los bloques, que pese a continuar emitiéndose cada 10 minutos, ahora serían capaces de albergar un número mucho mayor de transacciones, pasando de una tasa de aproximadamente 3,5 transacciones por segundo con 1mb de capacidad por bloque, a cerca de 24 transacciones por segundo gracias a dicha actualización en la que se pasan a 8mb por bloque (inicialmente, luego veremos que esta cifra es susceptible de aumentar). Por tanto, la principal propuesta de valor de esta criptomoneda es reducir tanto los tiempos de transacción como los costes derivados de ésta.

De los 8mb por bloque iniciales de este proyecto -que ya multiplicaban por 8 la cifra de transacciones del código de Bitcoin- en 2018 se decidió dar el salto a los 32mb por bloque lo que le otorgaría una capacidad para albergar unas 40.000 transacciones por bloque. Pese a que la escalabilidad es mucho mayor, a efectos prácticos en la realidad apenas logran ocupar el 5-10% de la totalidad de los bloques, por lo que la red se encuentra aún en crecimiento.

La capitalización actual de mercado es de unos 10 millones de dólares, quedando establecida como la número 12 de la lista de criptomonedas en base a su nivel de mercado quedando su precio unitario en 500$. Al igual que Bitcoin su tope de emisión se dispone en 21.000.000.

2.1.2.1 Ventajas y desventajas de Bitcoin Cash

Como puntos fuertes de esta criptomoneda encontramos:

- Al poseer un código muy similar al de Bitcoin, nos aseguramos de su elevado grado de seguridad y funcionalidad.
- Posee costes muy bajos y tiempos de transacción muy reducidos por lo que sería una herramienta transaccional muy buena.
- Ha sido ampliamente aceptada en el mercado, algo que se refleja con su avanzada posición en el mercado y en la cantidad de usuarios que tienen BTH en su cartera.

Por otro lado, los puntos débiles de esta moneda serían:

- En caso de que Bitcoin consiguiera superar sus problemas de escalabilidad mediante actualizaciones, BTH perdería significativamente utilidad y por tanto valor de mercado.

- Menor descentralización, ya que, para poder minar estos nuevos bloques más pesados, es necesaria también un mayor poder computacional y por tanto menos accesible para el público general.
- Es una red que aún tiene un número bajo de usuarios por tanto no se puede predecir su comportamiento, tiempos ni costes con tráfico intenso.
- Existen diversidad de opiniones tanto a favor como en contra de este *hard fork* por parte de miembros importantes de la comunidad de Bitcoin por lo que su situación aún es incierta.
- Posteriormente a Bitcoin Cash han aparecido nuevas criptomonedas con nuevos algoritmos que persiguen el mismo fin.

2.1.3 Monero (XRM)

Monero aparece en 2014 con la propuesta de crear una red en la que la privacidad y el anonimato consten como principal atractivo para sus usuarios y que además de esto, su código escapase de los cimientos creados por Bitcoin ya que esta emplea su propio algoritmo para asegurar que sus transacciones sean completamente anónimas.

Ilustración 12 Logotipo Monero

Fuente: crypto-economy.com

En este caso, Monero mantiene la seguridad propia de la Blockchain y del consenso para la aprobación de transacciones solo que ahora resulta completamente imposible rastrear cada transacción ya que estas se encuentran desvinculadas de los receptores, por tanto, la información queda registrada en la Blockchain pública, pero es imposible identificar a quien realizó la transacción.

En la actualidad, la capitalización total de Monero ha disminuido considerablemente desde la gran caída en mayo de todo el cripto-mercado quedando en 3.500.000$ para un precio unitario de 200$ con lo que ocupa la posición 25 del ranking global de criptoactivos.

En este caso Monero no cuenta con ningún tope de emisión, por lo que su creación es infinita.

Las principales ventajas de Monero son:

- Privacidad y anonimato totales, la base sobre la que se fundamenta esta criptomoneda. Mientras con otras monedas tanto nuestras transacciones como el saldo de nuestra cuenta se encuentran expuestos (y por tanto resulta posible asociar carteras a individuos) en Monero los usuarios pueden permanecer completamente separados de sus monederos y siendo un medio completamente legal de pago.

- Pese a mantener el anonimato y registrar todas las transacciones, la seguridad de su Blockchain y su protección frente a ataques es completamente sólida.

- Cuenta con una red de usuarios y programadores continuamente trabajando en ella y mejorándola.

Las desventajas propias de esta red serían:

- Esta criptomoneda ha sido muy vinculada con actividades delictivas ya que sus propiedades son ampliamente codiciadas por los ciberdelincuentes.

- Se han registrado varios casos de *malware* que ha infectado miles de equipos con el propósito de minar Monero sin que los propios dueños sean conscientes.

- Al no tener tope de emisión no se garantiza la tendencia alcista en su precio.

2.2 Criptomonedas relacionadas con la implementación de Smart contracts y aplicaciones descentralizadas

En este apartado quedan recogidas las principales criptomonedas cuyo protocolo es utilizado para almacenar contratos o aplicaciones inteligentes, autoejecutables y

descentralizadas. El fin de estas criptomonedas se centra en dar un servicio más allá de las criptomonedas que funcionan como divisa que vimos anteriormente.

2.2.1 Smart contracts y Dapps

Los Smart contracts, constituyen una de las creaciones digitales más relevantes en cuanto a utilidad se refieren de este siglo, estos consisten en una serie de instrucciones y acciones previamente especificadas que, al cumplirse ciertos requisitos, serán automáticamente ejecutadas.

Parten de la base del funcionamiento de los contratos convencionales, en los que se definen unos parámetros de actuación, consecuencias del incumplimiento, qué se permite y qué no etc…

Sin embargo, en el caso de los Smart contracts estos detalles se automatizan por completo gracias a la blockchain haciendo que estos sean más rápidos, baratos -al eliminar intermediarios como abogados o notarios- y fiables ya que también reducen los posibles "errores de interpretación" que podemos encontrar en los contratos convencionales. En un smart contract las acciones se graban en el script mediante comandos que se accionarán irrebatiblemente.

Además, estos códigos quedarán grabados en la blockchain de manera pública por lo que se asegura la transparencia y se guardara en infinidad de servidores distintos.

Las Dapps son muy semejantes con los Smart contracts en cuanto a sus características, pero guardan ciertas diferencias como por ejemplo la orientación que en caso de los contratos inteligentes se define claramente al mundo de las finanzas. En el caso de las DApps el campo de utilización es mucho más amplio y permite mayor variedad, al mismo tiempo las DApps también se ofertan para un número ilimitado, no definido, de usuarios en los que para los Smart contracts es un número determinado de partes. Éstas, además, a diferencia de las Apps convencionales, al encontrarse de manera descentralizada no dependen de un servidor central -como son las empresas que lanzan la aplicación- si no que son los usuarios de los que depende su funcionamiento.

2.2.2 Ethereum

Ethereum, fundada en 2015 por Vitalik Buterin, es la primera criptomoneda en ofrecer este tipo de servicios y nace con el objetivo de dar un servicio que permitiera dar soporte a aplicaciones descentralizadas y Smart contracts, de manera colaborativa y global.

El token con el que funciona Ethereum se denomina “Ether” (ETH) y pese a no poseer tope de emisión total, su inyección en el mercado se limita a 18.000 tokens anuales.

La blockchain de Ethereum funciona actualmente mediante PoW por lo que es necesario el trabajo de mineros para el funcionamiento de la red, en este caso cada bloque es generados en unos 14 segundos recompensando al creador con unos 5 ETH.

Actualmente, el Ether tiene la segunda mayor capitalización de mercado con cerca de 263.500.750.728$ y un valor unitario de algo menos de 2.300$, pero hace unos meses se encontraba cotizando entorno a los 4.000$ existiendo cerca de 112 millones de monedas en circulación actualmente.

2.2.2.1 Las DApps y Smart contracts dentro de Ethereum.

Ethereum, es la plataforma sobre la que se sustentan una inmensa cantidad de proyectos, tokens y aplicaciones, ya que esta actúa como medio para su desarrollo por parte de los usuarios que son quienes crean las instrucciones y programas que este debe ejecutar dentro de su blockchain. ETH no solo permite crear Smart contracts, al mismo tiempo permite crear tokens mediante el protocolo ERC-20, un protocolo estandarizado que permite la creación de tokens accesibles que pueden satisfacer las necesidades financieras de los proyectos que se quieran poner en marcha.

Algunas de las aplicaciones más conocidas desarrolladas sobre la plataforma de Ethereum serían:

El campo de las finanzas es el que más se ha desarrollado con la implementación de las DApps ya que además de permitir la creación de nuevos servicios, también puede mejorar la velocidad, eficiencia y seguridad de los ya existentes, por lo que se convierte en un medio abierto para cualquier proyecto que se nos ocurra:

- Aave: esta aplicación de finanzas descentralizadas permite prestar tus tokens con el fin de obtener intereses. Los objetivos principales de la plataforma son dos, en primer lugar, permite a sus usuarios invertir en pools para generar liquidez y de este modo permitirles prestar dinero a otros usuarios generándoles con ello unos intereses, además de esto, también permite configurar las opciones y políticas de colateralización para adaptarlos a sus necesidades.
- Oasis (DAI): este es otro ejemplo de DeFi, en este caso DAI nos da la posibilidad de prestar, pedir prestado, enviar y recibir dinero con comisiones casi inexistentes, pero además su principal particularidad es que el precio

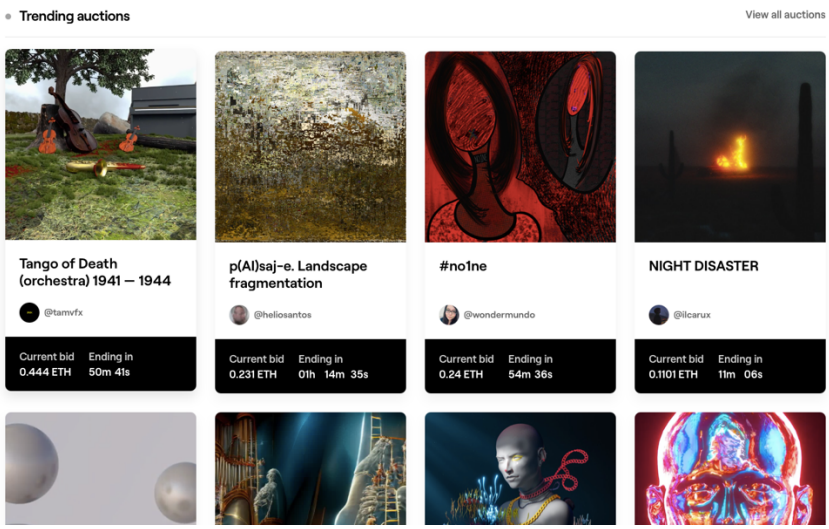
de su token se encuentra ligado al precio del dólar, por lo que soluciona uno de los grandes inconvenientes a los que se enfrentaba este mercado: la volatilidad. Por tanto, DAI se configura como la primera *stable coin* (que comentaremos en profundidad más adelante) configurada sobre Ethereum.

- Uniswap (UNI): aquí encontramos al mayor Exchange descentralizado del mundo de las criptomonedas, consiste en un sistema totalmente autónomo y de código abierto, entre las unciones que cumple Uniswap, se encuentran la de ofrecer servicios de intercambio y "swap" de criptodivisas además de permitirles crear un protocolo de liquidez automatizado, generando un fondo de liquidez que garantiza la máxima rapidez en las operaciones. Al tratarse de un programa descentralizado el control de los fondos siempre se encuentra en manos de los propios clientes, además asegura su compatibilidad con casi todos los tipos actuales de monederos
- Además de las aplicaciones mencionadas existe un variado abanico de posibilidades dentro del campo de las criptomonedas como por ejemplo "Nexus Mutual" una DApp encargada de asegurar tus productos financieros mediante Smart contracts, "Tornado Cash" que permite la realización de pagos instantáneos mediante Ether de forma completamente anónima y con mínimas comisiones o "Gitcoin Grants" un sistema de micro mecenazgo que permite financiar proyectos de manera grupal, descentralizada y completamente transparente.

En cuanto al mercado del arte y los coleccionables encontramos un mercado que ofrece la titularidad digital de obras además de la posibilidad de invertir en creadores y artistas abriendo las puertas a un nuevo mercado digital, algunos ejemplos de especial relevancia:

- Foundation: funciona como una plataforma de subastas destinada al arte digital, en ella artistas publican sus obras en formatos como imagen, video, gif etc… y los compradores adquirirán la titularidad de la obra mediante un token que garantiza su posesión, así como originalidad, el pago en esta plataforma se realiza a través de ether y toda ella está diseñada mediante contratos inteligentes.

Ilustración 13 Página Web de Foundation



Fuente: foundation.com

- Open Sea: funciona como la mayor plataforma mundial de compraventa de tokens NFT en el que los usuarios intercambian criptomonedas por tokens que pasarán a ser de su propiedad, el contenido de estos tokens puede estar sujeto a arte, tarjetas, coleccionables, música, incluso mundos virtuales… las posibilidades de tokenización son infinitas.

Actualmente también se han creado juegos basados en Ethereum, estos juegos son de alguna forma demostraciones del funcionamiento de la red, en ellos se crean mundos virtuales y coleccionables valorados en criptomonedas. Entre ellos se encuentran:

- CriptoKitties: Esta plataforma permite a los usuarios jugar e intercambiar tokens que contienen distintos gatitos animados. Los jugadores podrán crear diferentes gatos que serán únicos y de su pertenencia existiendo colecciones especiales y distintas rarezas. Este juego suscito polémicas en el pasado debido a que su elevada afluencia de juego puso en duda la escalabilidad del proyecto Ethereum al no poder dar salida a la demanda de operaciones que trajo consigo esta DApp.
- Decentraland: es un juego de simulación en el que, en un mundo virtual, puedes comprar “terrenos virtuales” y construir sobre ellos todo lo que se te ocurra, sin ningún tipo de límite para los usuarios, además todo lo que crees dentro del juego te pertenecerá a ti en

exclusiva, no a una entidad central. El juego cuenta con un token propio el *MANA* basado en ERC20 que es la moneda con la que podremos comprar terrenos dentro del juego para poder hacerlos de nuestra propiedad.

Ilustración 14 Decentraland

Fuente: invdes.com

En el campo de la tecnología descentralizada, Ethereum ofrece herramientas descentralizadas que ofrecen nuevas e interesantes posibilidades a los desarrolladores:

- Golem: Esta herramienta, nos permite el acceso a una red de préstamo de potencia informática compartida por otros usuarios de la red que deciden poner a disposición de la red os recursos de trabajo que no estén utilizando y con ello brindar soporte a aquellos desarrolladores que necesiten disponer de mayor capacidad de computación de manera puntual sin necesidad de que adquieran equipos avanzados para ello.
- Opera: opera es un buscador web que permite integración con monederos y sistemas de criptomonedas en su interfaz. Aseguran mejorar la velocidad, la optimización de recursos y la protección del usuario y además de esto permiten operar con tus criptomonedas y sus ecosistemas en tus actividades del día a día, haciendo que trabajar con ellas sea mucho más sencillo de lo que lo era en el pasado.

Y estas son algunas de las posibilidades que existen actualmente en la red Ethereum, que como podemos comprobar las posibilidades que nos brinda este sistema son amplísimas y pueden dar servicio a un sinfín de las necesidades, es por eso que Ethereum como tal no es tanto una criptomoneda sino más bien una plataforma de creación basada en Blockchain y su token el Ether es la que cumple con las funciones monetarias.

2.2.2.2 Las actualizaciones de Ethereum

Como casi cualquier proyecto es prácticamente imposible acertar con todos los parámetros desde el primer día de su creación, por el camino surgen imprevistos o nuevas necesidades o oportunidades de mejora, es por este motivo que Ethereum se encuentra en proceso de evolución.

En primer lugar, debemos identificar cuáles son los fallos o inconvenientes que encontramos en la red actual.

El primer y más sonado problema que nos plantea Ethereum es su escalabilidad ya que esta red ya se ha visto en varios casos sobre congestionada por no poder dar salida a la numerosas y crecientes transacciones que se ejecutan sobre ella, como por ejemplo en el ya comentado caso relacionado con *Criptokitties* donde la red colapso debido al cuello de botella que se formó durante el boom de esta DApp. En la actualidad, puede dar soporte a de 15 a 45 transacciones por segundo lo que se queda algo corto a la hora de dar salida a la demanda existente. La solución impuesta temporalmente (a modo de parche) para este problema ha sido el encarecimiento de los costos de transacción. Además de esto, el programa depende de los nodos que forman parte de su sistema para subsistir, estos quedan Inter conexionados y son los que permiten actualizar la red, a los desarrolladores no les interesa dejar la plataforma en manos de solo unos pocos nodos de grandes dimensiones que podrían ser atacados o monopolizar parte del sistema ya que perdería una parte importante de su descentralización.

Por esto, para la actualización del sistema, se comenzó el desarrollo de Ethereum 2.0 que tiene como objetivo mejorar la escalabilidad, fluidez y seguridad de la plataforma. Esto pretenden conseguirlo añadiendo 64 cadenas nuevas al sistema de forma que la carga de información sea mucho menor y más accesible, de esta forma será un ecosistema mucho más descentralizado que su versión anterior y por ende también mejorara su seguridad. Además, como plato fuerte, propone la eliminación de la minería mediante PoW para dar pie a un sistema de *Staking* que mejorara enormemente no solo la escalabilidad del sistema, sino también la eficiencia en términos energéticos de su funcionamiento.

La puesta en marcha de esta actualización ya ha comenzado a llevarse a cabo, mediante la primera fase de incorporación de la denominada “Cadena de Baliza” que pretende asentar el camino para las dos fases venideras: la “Cadena de fragmentos” prevista para ser añadida a lo largo de este año y el “Acoplamiento” con la que veremos finalizada esta actualización en algún momento de 2022.

2.2.2.3 ¿Qué ventajas e inconvenientes nos propone Ethereum?

Las principales ventajas que ofrece esta plataforma serían:

- Dentro de su campo es la moneda con mayor trayectoria y capitalización, en el ámbito de los contratos inteligentes se declara absoluta vencedora y sirve de soporte para las principales aplicaciones existentes actualmente en el mercado, además también ocupa la segunda posición en cuanto a capitalización de criptomonedas de todos los tiempos.
- Se encuentra abierta a continuas mejoras y actualizaciones lo que la permite adaptarse con soltura a los nuevos requerimientos del mercado como es el caso de ETH2.
- El equipo detrás de esta es uno de los más brillantes del segmento y cuentan con el apoyo y el soporte de empresas punteras de todo el mundo.
- Es ampliamente aceptada por diversas compañías en varios sectores industriales.
- Gran parte de los proyectos con mayor potencial en el futuro se encuentran basados en Ethereum.
- Es una plataforma que permite la creación de nuevas monedas sobre ella.

En cuanto a los puntos débiles que puede presentar, encontraríamos:

- Una de las particularidades que presentan los Smart contracts que, si bien puede verse en muchos casos como una ventaja, en otros puede ser un grave problema es la irreversibilidad de estos, que una vez ejecutados al ser algo automatizado no permiten deshacer los efectos.
- La situación anterior se agrava si existe algún fallo en los Smart contracts, ya que, al ser bastante complejos, es fácil cometer una equivocación y que esta pueda suponer grandes problemas o pérdidas de dinero.
- Al formar parte de un mercado tan volátil y especulativo como es el de las criptomonedas, es frecuente ver grandes variaciones en el precio que pueda provocar inseguridad a la hora de operar a los usuarios.

- Aunque cada vez más accesible, sigue siendo una tecnología compleja para el público poco familiarizado con ella.

2.2.3 Cardano

Cardano es un revolucionario sistema de blockchain basado en *proof of stake* que presume de haber podido aprender de los errores de sus antecesoras y pretende brindar un nuevo nivel de tecnología, escalabilidad y seguridad.

Ilustración 15Logotipo de Cardano

Fuente: profesionalreview.com

Cardano es la primera red blockchain a nivel mundial considerada “científica”, esto se debe a la comparación que lleva a cabo con Bitcoin, ya que la primera criptomoneda salió al mercado partiendo de un autor desconocido que aglutino varias tecnologías en un proyecto y lo puso a disposición de la sociedad sin ninguna clase de revisión del proyecto o búsqueda de mejoras (que tuvo que llevarse a cabo por parte de la comunidad). Otras criptomonedas pese a si mantener interés en comprobar cómo se desenvuelve su proyecto, en primera instancia actúan mediante prueba-error sin una revisión científica realmente certera, este no es el caso de Cardano, que emplea el método científico para absolutamente cualquier acción que pretenda llevar a cabo, desde su *whitepaper* hasta la evaluación del rendimiento de la plataforma.

Esta moneda fue desarrollada por Jeremy Wood y Charles Hoskinson (Cofundador de Ethereum) quienes a finales de 2017 minaron el primer bloque de Cardano y obteniendo las primeras recompensas en “ADA” su token propio. Cardano se considera una Blockchain de tercera generación, lo que significa que puede ser transmisora de valor, ejecutar Smart contracts y además gracias a su diseño en arquitectura modular es posible su posterior reajuste.

Emplea el sistema “Ouroboros” como algoritmo de consenso, esto es una variante del ya conocido PoS, que mediante combina la revisión de los participantes con complejos algoritmos para su verificación. Gracias a este nuevo sistema Cardano emite un bloque cada aproximadamente 20 segundos y presume de mejorar la eficiencia energética a la par que la seguridad.

Cardano ha decidido fijar su emisión máxima en 45.000 millones de unidades de las cuales el 71% se encuentran emitidas ya (alrededor de 33 mil), ocupa el puesto 5 en cuanto a capitalización total de mercado con más de 42 billones de dólares y un precio unitario marcado en este momento a 1,32$.

2.2.3.1 El desarrollo de Cardano

El funcionamiento de Cardano como ya hemos comentado permite emplearlo como medio para la realización de transacciones económicas o bien para cargar en su red Smart contracts por lo que su objetivo es desbancar a Ethereum y Bitcoin como líderes.

En la actualidad es un programa que aún necesita mucho desarrollo si pretende lograr sus ambiciosos objetivos, esta evolución se muestra en las continuas actualizaciones que recibe además de en el detallado “roadmap” o plan de ruta que plantea, en el que se especifican diversas fases en las que ira implementando todas las funcionalidades planteadas a su programa. Estas implementaciones se realizarán siguiendo las distintas etapas del proyecto. Actualmente la fase *Byron* esta completada y nos encontramos en la *Shelley* en la que se implementa el algoritmo “Oroboros” en la siguiente fase *Goguen* los Smart contracts serán implementados finalmente en Cardano otorgándole por fin la mayor parte de las funcionalidades más reclamadas por los usuarios.

Después de esta solo faltarían las fases *Basho* y *Voltaire* en las que se esperan mejoras en el rendimiento y un asentamiento final de la red autogestionada.

2.2.3.2 Ventajas y desventajas de Cardano

Cardano propone interesantes ventajas para los futuros mercados como pueden ser:

- En primer lugar su organización, Cardano sigue un detallado *roadmap* en el que se desarrolla una idea muy compleja a la perfección sin dar cabida a posibles imprevistos, por lo que en este sentido es una de las criptomonedas mejor elaboradas.

- Su equipo de trabajo con ex miembros de la plataforma Ethereum está altamente experimentado en estas tecnologías, además cuentan con el importante respaldo de grandes académicos que apoyan fehacientemente la criptomoneda.
- Cardano emplea varias capas en su blockchain designadas a las transacciones y a la parte computacional, que garantizan su escalabilidad y buen funcionamiento.
- Su nuevo sistema de verificación "Ouroboros" es muy prometedor y perfecciona el ya existente protocolo de *Staking* mejorando su eficiencia y seguridad.
- Es una red muy actualizada, que se encuentra en continuo proceso de aprendizaje y mejora. Poniendo especial atención a las necesidades de sus usuarios.

En cuanto a los problemas que puede plantear esta red en la actualidad:

- El primer y más importante problema es su escasa madurez como proyecto, aún se encuentra en una fase muy temprana de desarrollo y su progreso se observa lentamente por lo que a estas alturas resulta imposible predecir el futuro de la criptomoneda.
- Muchos expertos aseguran que en la actualidad es una cadena frágil y vulnerable, debido a su inmadurez lo que supone un problema para muchos inversores.
- Con la aparición de las últimas propuestas de criptomonedas, su sistema, aunque útil ya no resulta tan innovador como lo parecía en un primer momento.
- Existen ciertas rivalidades y diferencias con el equipo desarrollador de Ethereum, que pueden dar lugar a problemas y controversias entre ambos.

2.3 Otras criptomonedas de interés.

Este apartado queda reservado a aquellos proyectos de moneda que plantean beneficios particularmente interesantes dentro del mundo de las "criptos", debido a que hay infinidad de propuestas de un asombroso valor e interés general, me limito a exponer solo

algunas de ellas con el fin de no alargar en exceso el presente trabajo, por tanto, son todas las que están, pero no están todas las que son.

2.3.1 Ripple

Esta moneda se creó con la intención de destituir las actuales transacciones bancarias y su principal utilidad es la de mover fondos entre cuentas de cualquier lugar del mundo, reduciendo al mínimo los costes operativos y por supuesto con la mayor seguridad posible.

Ripple funciona como una plataforma de pagos y cambio de divisas internacional, su particularidad es la gran capacidad de transacciones por segundo (aproximadamente 1.000/s). Gracias a esa fluidez es por lo que es la gran favorita de muchos Bancos y empresas. Además, posee una larga trayectoria pues desde sus inicios en 2004 como un programa básico de pagos, pasando en 2011 por la creación de un sistema financiero virtual básico a la actualidad en la que se conforma como una criptomoneda con blockchain propio ha sido aclamada por bancos y empresas de renombre.

Su oferta se encuentra dirigida a bancos y demás instituciones financieras, entre las que sirve de intermediario para la ejecución de cobros y liquidación de transacciones,

Es una criptomoneda peculiar, en este caso encontramos que toda la emisión monetaria de Ripple (conocida como XRP) ya ha sido creada, alrededor de 100.000 millones dando como resultado que pueda mantener siempre una inflación igual a 0.

El tráfico de esta moneda se administra por la propia empresa de Ripple por lo que es una criptomoneda centralizada que es susceptible de ser controlada por la empresa a su cargo, lo que puede tener consecuencias negativas como puede ser caer en la manipulación o actuar según intereses particulares, pero también le otorga importantes beneficios a la hora de ser gestionada o en cuanto a su escalabilidad y dado el fin con el que ha sido creada, su estructura fomenta el adecuado funcionamiento de la misma.

2.3.2 Tether

Esta criptomoneda tiene un funcionamiento muy peculiar ya que se engloba dentro de las conocidas como “Stable coins” o monedas estables, y es que su rasgo caracterizador, es que su valor se encuentra lejos de las grandes fluctuaciones que pueden presentar otras criptomonedas de la lista y esto es debido a que su valor se encuentra asociado al del dólar. Al quedar su valor parejo al dólar, (en principio) no se le esperan fuertes variaciones en el precio dentro del corto plazo, por lo que es idónea para realizar

transacciones sin riesgo. Esta paridad la consigue manteniendo una reserva de 1:1 en dólares en su cuenta bancaria (lo cual hoy en día suscita dudas entre sus inversores ya que aún no han sido presentadas auditorias completas por parte de la compañía).

La abreviatura de Tether es USDT y el valor de sus transacciones en el mercado representa aproximadamente tres cuartas partes del comercio total que genera Bitcoin siendo así una de las principales criptodivisas del ranking.

Entre las mejores aportaciones de Tether encontramos:

- Permite aplicar todas las ventajas de una criptomoneda (universalidad, comisiones, seguridad etc..) a una divisa tradicional como es el dólar.
- Plantea una forma de protección para los inversores dentro del Exchange al no estar obligados a guardar su capital en una criptomoneda volátil.
- Al mismo tiempo también ofrece una forma de pago segura para los consumidores que deseen emplearla como medio de pago.

2.3.3 Polkadot

Esta es otra de las criptomonedas peculiares que busca revolucionar el sistema actual de criptomonedas, en su caso plantea la posibilidad de generar una red unificada que incorpore varias blockchains.

Con la aparición de la web 3.0 y las criptomonedas de tercera generación se buscaba una forma de que las blockchains pudieran actuar de manera conjunta, partiendo de este *target,* Polkadot creó un entorno que permitiera dicha interoperabilidad entre diversas blockchains existentes, proporcionar un elevado grado de fluidez debido a que según su programación es capaz de realizar varias operaciones de manera simultánea y permitir a las blockchains mantener su sistema de gobernanza original aunque se encuentren unificadas.

Una de las funciones más innovadoras que nos ofrece es posibilitar a las criptomonedas implementar actualizaciones sin necesidad de producir bifurcaciones (creando otra criptomoneda diferente a la original).

Finalmente proporciona un medio de validación interno más sostenible y optimizado con lo que resolver muchos de los problemas medioambientales generados por las criptomonedas más antiguas.

2.3.4 VaCoin

A través de la iniciativa Valladolid Blockchain, el experto en criptomonedas vallisoletano Carlos Callejo, inició este proyecto de criptomoneda con el objetivo de desarrollar proyectos en los que se pueda utilizar esta moneda, y así, comprobar su potencial.

Ilustración 16 Logotipo VaCoin

Fuente: criptonoticias.com

Entre las propuestas que nos hace este proyecto se encuentran la elaboración de un sistema de pagos reales, un sistema más actualizado de votación y otras aplicaciones que permitan su implementación con esta criptomoneda vallisoletana, según cuenta su creador no quiere poner límites al ámbito de uso de este activo por lo que está dispuesto a ampliarlo a cualquier entorno donde pueda ser útil esta tecnología.

3 Proyecto de elaboración de una criptomoneda

Como parte práctica del presente trabajo y con intención de mostrar la accesibilidad actual que presentan las criptomonedas, dado que como veremos no serán necesarios conocimientos muy extensos sobre criptografía o informática, voy a mostrar el proceso de configuración y creación de una criptomoneda propia generada de manera real aunque con intenciones ficticias. Mi intención es que funcione como una moneda de intercambio y recompensa para profesores, alumnos y otros integrantes de la facultad de Comercio de Valladolid.

Primeramente, definiremos cual es el objetivo, o más bien, la finalidad con la que nace esta moneda. La premisa de este nuevo criptoactivo reside en la posibilidad de implementar un sistema interno de pagos, recompensas y cooperación.

Nuestro público objetivo será cualquier estudiante, profesor o partícipe de la Facultad de Comercio de Valladolid, y será únicamente operable por aquellos usuarios que demuestren su relación con la facultad, pues el acceso al monedero de criptomonedas correspondiente quedará restringido a este target potencial.

A continuación, debemos seleccionar el proceso de creación que vamos a emplear.

Debido a que como ya se ha mencionado anteriormente, nuestra intención es la accesibilidad y facilidad de creación, evitaremos el proceso de desarrollo de una Blockchain única y propia de esta criptomoneda. Para ello emplearemos una plataforma que nos facilita el proceso realizando nuestra blockchain basada en el código abierto de una preexistente.

En este caso la plataforma que utilizaremos para este proceso es: https://www.walletbuilders.com. En esta página podremos crear nuestra moneda cómodamente asignando los valores que creamos oportunos y posteriormente generar un blockchain basado en un algoritmo de nuestra elección.

Ilustración 17 Logotipo de WALLETBUILDERS

Fuente: walletbuilders.com

Seguidamente pasamos al proceso de designación de los parámetros necesarios para la creación de la moneda en base a los objetivos y funcionalidades que esperamos obtener de ésta. En la primera pestaña seleccionaremos los apartados básicos: nos solicita un correo electrónico (para enviarnos un link a nuestro monedero), el tipo de moneda que queremos crear -de pago o gratuita- y finalmente el protocolo sobre el que queremos construirla:

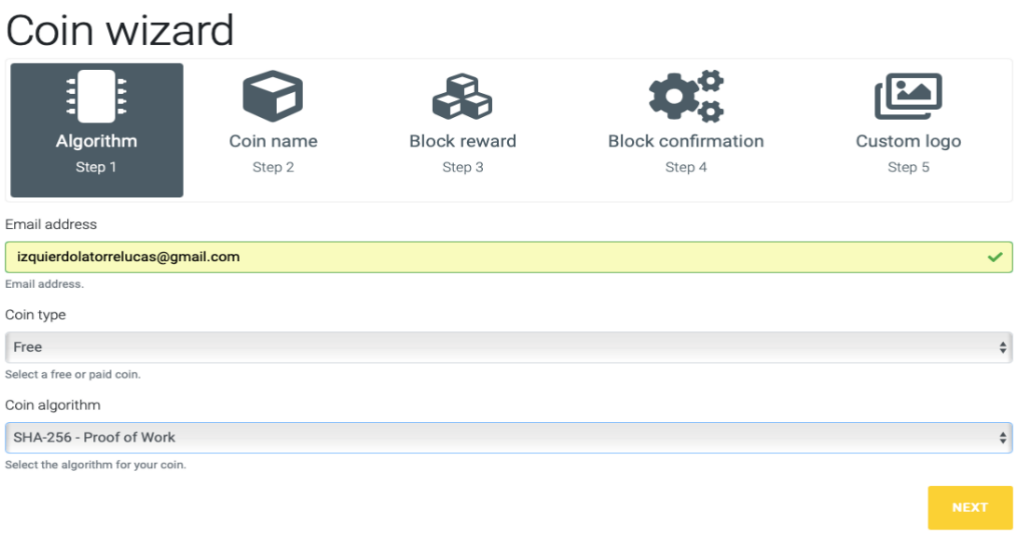
- Scrypt- PoW
- Scrypt- Pow y PoS
- SHA-256- PoW
- X11- PoW y Master Node
- Quark- PoW, PoS y Master node

Los protocolos “Scrypt” son los empleados por plataformas como Litecoin o Dogecoin y presume de ser un protocolo sencillo y con un proceso de seguridad potente basado en contraseñas, dentro de las opciones que nos permite “Scrypt” se encuentran tanto la prueba de trabajo (Litecoin) como la de participación (Blackcoin).

El protocolo SHA-256 consiste en una de las opciones de trabajo más sólidas y seguras de todas, pues es en la actualidad el mismo protocolo que se emplea en el *hasheado* de Bitcoin que utilizará la prueba de trabajo como forma de verificación, los protocolos X11 (correspondiente a la criptomoneda Dash) y Quark (propio de la criptomoneda con este mismo nombre) nos ofrecerán funciones mucho más avanzadas debido a su algoritmo más moderno y complejo y permitirán crear una jerarquía de nodos dentro del sistema.

En vista de las necesidades particulares de este proyecto y teniendo en cuenta su uso y búsqueda de sencillez, el protocolo que emplearemos será el SHA-256 debido a su sencillez, robustez y mecanismo de funcionamiento ya que los protocolos X11 y Quark son excesivamente complejos de operar y minar además de que no nos reportan beneficio alguno frente al SHA-256. En cuanto a las plataformas Scrypt también las rechazaremos debido a que en nuestro caso el sistema más “semejante” a Bitcoin (el SHADOW-256) es el que vamos a emplear para esta demostración.

Ilustración 18 Creación de una Criptomoneda I



Fuente: walletbuilders.com

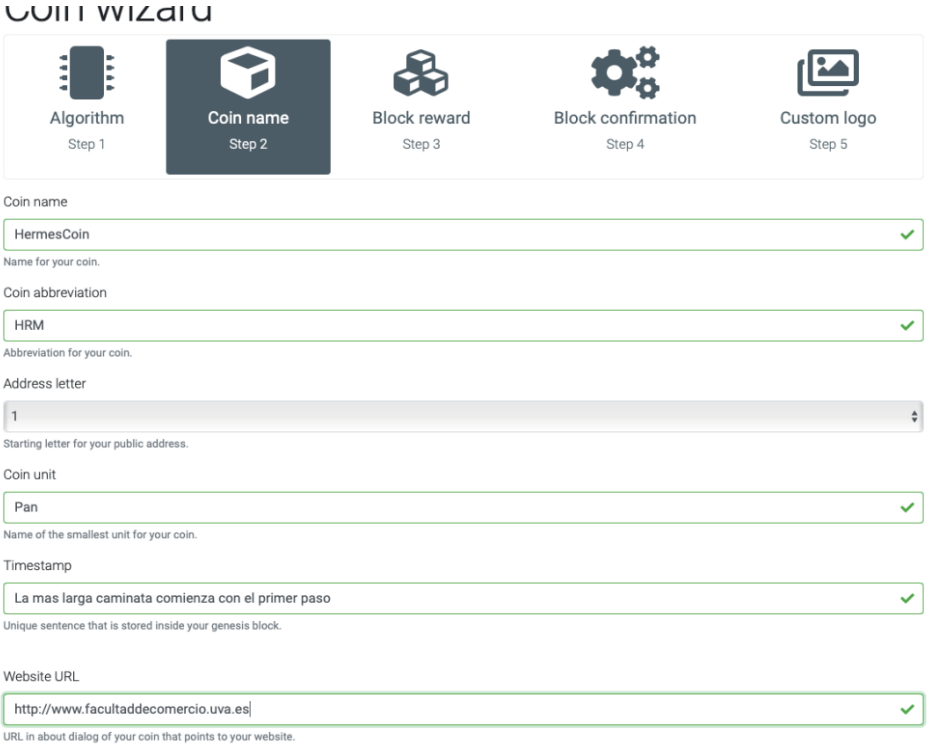
Ahora llega el momento donde deberemos decidir el nombre con el que será bautizada la moneda. En mi proyecto decidí apodarla ***HermesCoin*** haciendo un guiño a la mitología griega en la que así era llamado el dios del comercio. También deberemos indicar la abreviatura con intención de facilitar su manejo, en forma de acrónimo, he elegido **"HRM".** El "Adress letter" es el número por el que comenzarán las direcciones públicas, este número es completamente indiferente por lo que lo dejaré por defecto en 1.

La "Coin unit" hace referencia al nombre que recibirán las subunidades o unidades menores de la criptomoneda, algo así como los "céntimos". El creador de Bitcoin denominó a los suyos "Satoshis". En este caso por seguir con la tónica mitológica se llamará: ***Pan***, como uno de los hijos de Hermes, destacando de este nombre su simplicidad y facilidad de escritura.

El "Timestamp" es quizá una de las partes más "poéticas" de las criptomonedas, aquí se debe introducir un texto de aproximadamente 70 caracteres que conformará el contenido del primer bloque o bloque génesis, esto es necesario para poder obtener un hash que sirva de nexo con los siguientes bloques, aunque no tiene relevancia técnica alguna cual sea el contenido de este. A modo de curiosidad, Satoshi utilizo un titular del periódico "The Times" con fecha del 3 de enero de 2009 asegurando que ninguna moneda con anterioridad a esa fecha pudo ser minada, en el artículo se mencionaba la caída de los bancos. En mi *Timestamp* decidí poner una frase, que para mí representa un poco el

sentido de las criptomonedas: **"*La mas larga caminata comienza con el primer paso*"** *(*no permite el uso de acentos ni signos de puntuación). Finalmente nos deja un recuadro para añadir una dirección URL para nuestra página web, en este ejemplo la de la facultad de Comercio.

Ilustración 19 Creación de una Criptomoneda II



Fuente: walletbuilders.com

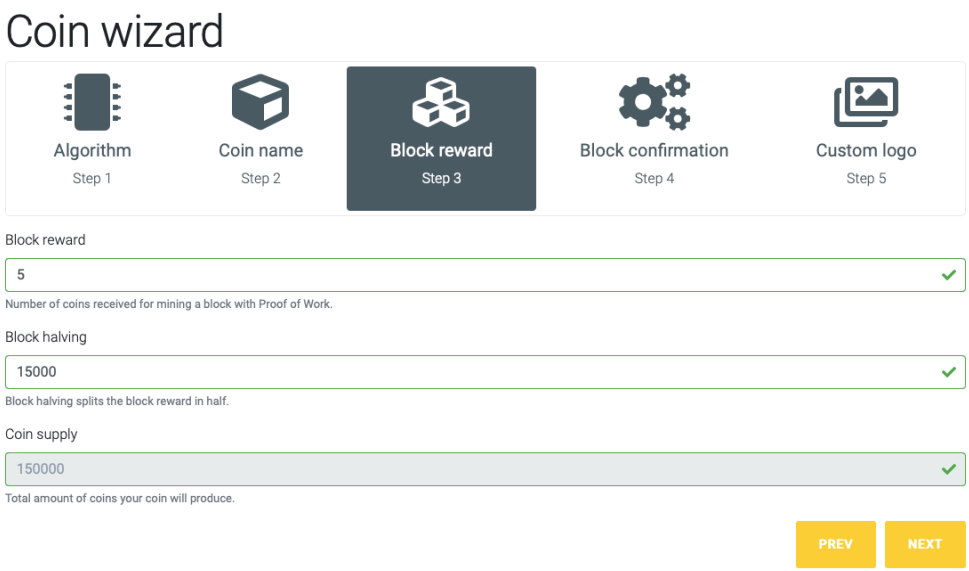
En la siguiente pestaña nos encontramos en primer lugar con la recompensa por bloque (Block reward), aquí debemos indicar cual será la recompensa en unidades monetarias que en este caso recibirán nuestros mineros cada vez que logren minar un bloque, para este protocolo decidí establecer una recompensa de 5 unidades de la moneda en vista de hacer sencilla su operación real con esta moneda (que no se tenga que trabajar con cifras disparatadas).

En el marcador del *halving* decidiremos el bloque en el que se dividirá la recompensa entregada a los mineros como ya hemos comentado para limitar la oferta de la criptomoneda, en nuestro proyecto lo determinaremos en 15.000.

Por último, falta decidir el número total de criptomonedas que podrán ser emitidas que como se trata de una moneda para un número "relativamente" reducido de usuarios

quedara dispuesto en 150.000, este dato lo elige automáticamente la página en función del *halving.*

Ilustración 20 Creación de una Criptomoneda III



Fuente: walletbuilders.com

En la última sección en cuanto a configuración de los parámetros básicos se refiere encontramos:

La “Coinbase maturity”. Esta es una característica de seguridad que se implementa en algunas criptomonedas, su función consiste en retener las criptomonedas entregadas a los mineros hasta cumplir cierta cantidad de confirmaciones sobre ellas, el objetivo es aumentar la seguridad y eliminar posibles gastos duplicados. Para nuestra moneda lo vamos a establecer en 5 en vista de no hacer demasiado tedioso este procedimiento para nuestros mineros.

El “Number of confirmations” como su propio nombre indica serán el número de confirmaciones necesarias para que la transacción sea válida. Lo más adecuado para nosotros sería mantenerlo en 3 para sin demorarlo demasiado, poder mantener un buen nivel de seguridad en la red.

En cuanto al “Target spacing in minutes” y al “Targuet timespan in minutes” son los valores de tiempo que se tardará en minar y en reajustar la dificultad de minado respectivamente de nuestra moneda, en mi opinión para nuestra moneda considero que lo

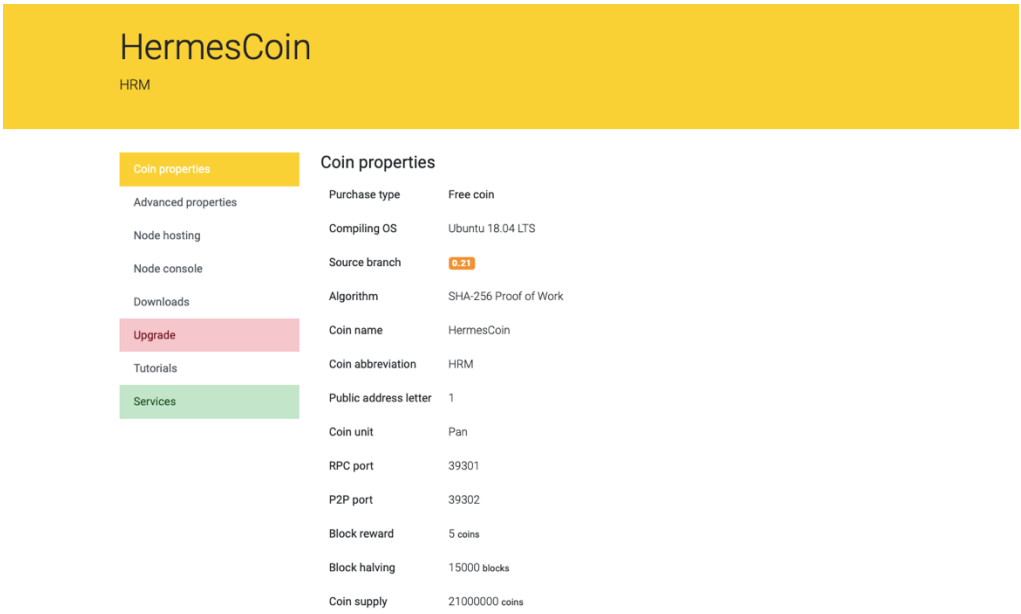
más adecuado es mantenerlo en los valores de 3 y 6 minutos teniendo en cuenta el volumen estimado de la red y la velocidad a la que queremos inyectar monedas al sistema.

El resto de los parámetros hacen referencia a los nodos principales y sus direcciones de servidor, como nosotros trabajaremos con los propios de *WalletBuilders*, los vamos a dejar con las opciones predeterminadas.

Si hubiéramos seleccionado la versión de pago a la hora de crear la criptomoneda, tendríamos un apartado más en el que podríamos añadir un logo a la misma, pero como el proyecto es por el momento una demostración no estimé oportuno hacer el desembolso por las funciones añadidas que nos ofrece la opción Premium.

Una vez hecho esto pasada una hora nos llegará un correo con un link para acceder al directorio de nuestra moneda, de donde podremos descargar el monedero para la criptomoneda, además podremos ver toda la informacion referente a la misma.

Ilustración 21 Creación de una criptomoneda IV



Fuente: walletbuilders.com

Esta criptomoneda, a efectos prácticos funciona como un token, es decir, como un sistema de recompensas/pagos a nivel interno en una comunidad.

3.1 Primeros pasos con nuestra criptomoneda.

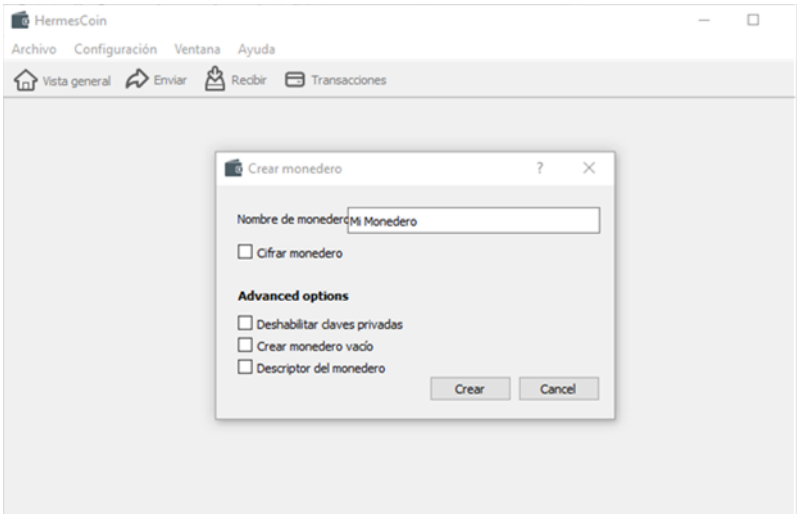
Una vez establecido el primer nodo y habernos descargado el monedero de la criptomoneda podremos comenzar a minarla para obtener las primeras recompensas.

Aquí tenemos el link para cualquiera que desee descargar el monedeo:

https://www.walletbuilders.com/mycoin?coin=ebeb1204cff5318acf566a6d968eec03d952dc57216deea706

Ahora crearemos nuestra primera cartera:

Ilustración 22 Creación de una criptomoneda V



Fuente: Elaboración propia

Ya tenemos nuestro monedero, pero aún no existe ninguna moneda minada en nuestra red. El minado se realiza mediante comandos en la consola del ordenador, mientras estemos minando, se emplearán los recursos de la CPU para obtener *hashes* la dificultad de minado se ajustará automáticamente con la potencia de la red para que tarde siempre alrededor de 3 minutos.

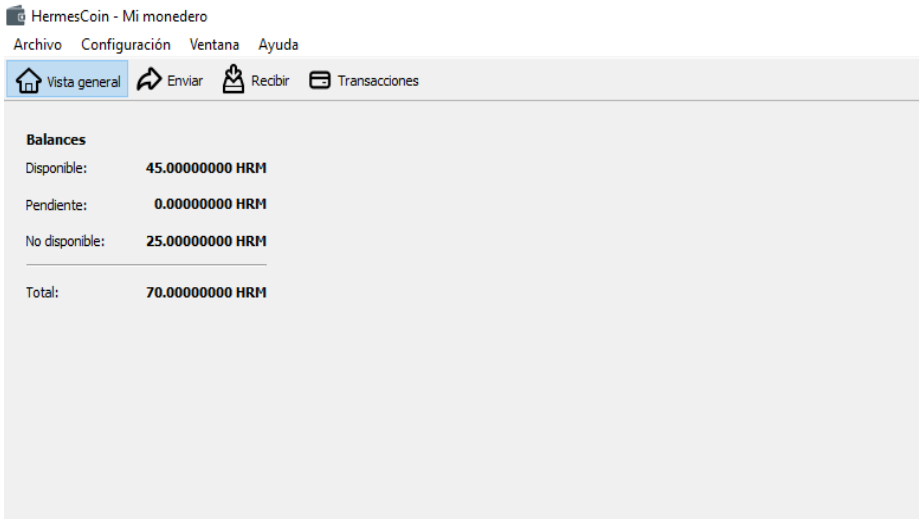
Este es un ejemplo de la consola cuando logra minar un bloque:

Ilustración 23 Creación de una criptomoneda VI

Fuente: elaboración propia

Tras el minado se sumarán -5 HRM- a nuestro monedero, que nos mostrará el total de monedas de las que disponemos

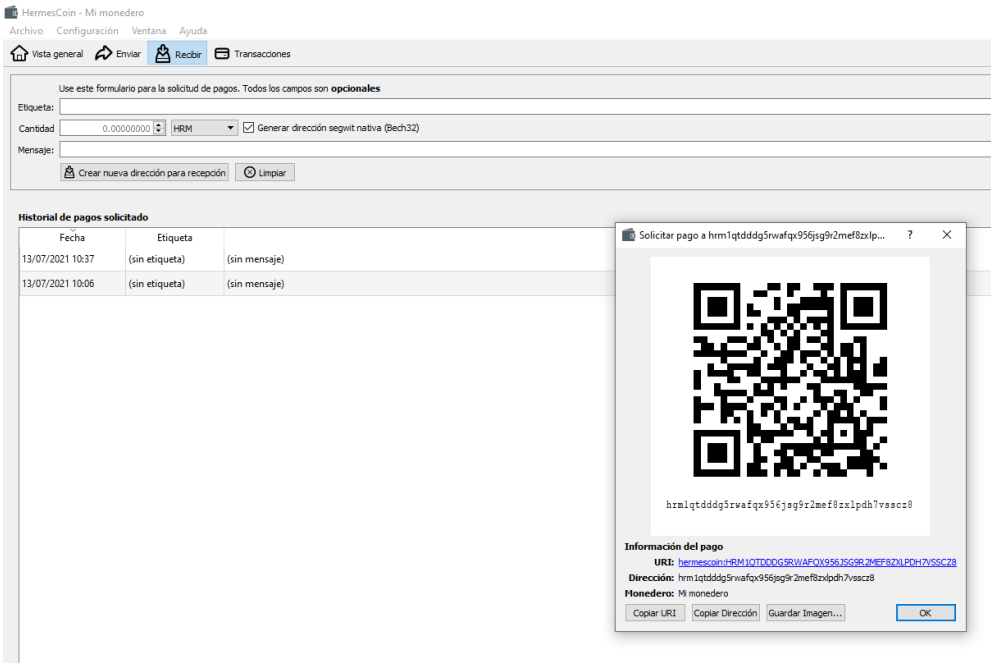
Ilustración 24 Creación de una criptomoneda VII



Fuente: elaboración propia

En este punto, ya disponemos de nuestra criptomoneda y podremos realizar y recibir pagos con ella, el monedero nos permite tanto enviarlo a otra dirección de monedero o bien nos generará un código para que otras personas puedan transferirnos monedas a nosotros.

Ilustración 25 Creación de una Criptomoneda VIII



Fuente: elaboración propia

3.2 ¿Qué utilidades tiene?

Si bien si bien su utilidad se ve un poco mermada al solo poder intercambiarse desde monederos instalados en ordenadores, por ejemplo, no disponemos de app para el Smartphone (opción que si permite la versión de pago).

Si esta red adquiriese un volumen de relevancia y una propuesta de valor interesante, podría ser inscrita en algún exchange para su puesta a disposición del público general, para entenderlo mejor: este producto es como una marca de camisetas, nosotros podemos venderla desde nuestro puesto en por ejemplo una feria o mercadillo, pero si queremos que esta sea comercializada en grandes cadenas de tiendas de ropa será necesario que los clientes la demanden y la marca crezca lo suficiente para que sea aceptada en esos comercios.

Su principal utilidad está claro que sería la de enviar y recibir pagos, ya que posee todas las ventajas que podemos cualquier otra criptomoneda existente, pero en cuanto a nuestro caso particular, he decidido aportar algunas ideas sobre como aumentar el valor de la moneda:

- En primer lugar, puede emplearse como un medio para aumentar el grado de implicación de alumnos y profesores en la facultad, esto se conseguiría estableciendo un sistema de recompensas por llevar a cabo determinadas acciones, estas acciones pueden ser la asistencia o preparación de conferencias, prestar ayuda durante ferias o exposiciones, realizar actos de promoción en nombre de la facultad, revisar documentos para la biblioteca etc…
- También puede premiarse la consecución de logros tanto académicos como personales con una suma de criptomonedas: Obtención de matrículas de honor, victorias en el trofeo rector y otros méritos de especial relevancia.
- Los alumnos pueden recibir a cambio de sus monedas descuentos en reprografía, acceso a conferencias o eventos especiales, descuentos en actividades deportivas etc…
- La posibilidad de colaboración con VaCoin, al ser los dos tokens digitales, podría contemplarse la opción de permitir *swaps* con la criptomoneda Vallisoletana.

  Además esta moneda beneficiaria activamente a la facultad en varios aspectos que considero muy interesantes, ya que por ejemplo gracias estas posibles recompensas todos los integrantes de la red aumentarían su grado de compromiso con la facultad en una relación de mutuo beneficio en las que ambas partes obtienen una ganancia, así mismo también mejoraría notablemente la posición de la facultad al establecerse como pionera en implementar este tipo de tecnología en su estructura, lo que la concedería una posición de referencia a nivel nacional e internacional. No podemos olvidar tampoco el hecho de que los alumnos aprenderían mediante su propia experiencia (que es la forma más efectiva) sobre el funcionamiento de esta tecnología, que, de cara al futuro, será una competencia deseable por muchas empresas.

4 Conclusiones

Considero que, tras esta aproximación conceptual y funcional al mundo de las criptomonedas, creo haber logrado una mayor comprensión sobre el tema tanto de saber, como de saber hacer, pero me queda la duda si es comprensible para un lector no iniciado en el tema, dada su complejidad y extensión.

A pesar de haber comprobado que la dificultad de esta tecnología superaba con creces mis expectativas previas, también puedo afirmar que cuanto más he podido aprender de éstas, más convencido estoy de sus increíbles aplicaciones en la sociedad contemporánea.

Las criptomonedas han venido para quedarse, y prueba de ello es que, es un mercado en continua evolución debido continuas incorporaciones de proyectos y nuevas utilidades. Así mismo tampoco podemos obviar el hecho de que hoy en día sigue siendo un mercado complicado, de extrema volatilidad y que aún se encuentra en desarrollo.

Como cualquier gran acontecimiento en la historia, los inicios son lentos y en este caso aún queda una larga caminata hasta su aceptación y normalización global.

Tras toda la recopilación de información llevada a cabo, se me abre el apetito de querer aplicarla a algo funcional que pueda desarrollar en mi quehacer profesional -especialmente el tema de las aplicaciones construidas sobre las bases de Ethereum y Cardano- así espero con avidez sus futuras actualizaciones y ver que les depara el futuro a estas dos criptomonedas con muchas potencialidades.

He disfrutado enormemente con la creación de mi propio proyecto de moneda, en el cual espero seguir trabajando hasta comprender al detalle los entresijos de su funcionamiento y con toda probabilidad desarrollaré una versión actualizada de este token para explorar todas sus posibles utilidades y aplicaciones. También considero que debo formarme con mayor incisión en cuestiones de programación y lógica para comprender mejor cada uno de los procesos que he debido realizar para producción final de la moneda.

En cuanto a las principales dificultades encontradas, destacaría en primer lugar, que muchas de las características de estas redes responden a ramas matemáticas e informáticas que escapan de mis capacidades teniendo que emplear una gran parte del tiempo en comprender nuevos términos e ideas. Me gustaría resaltar la dificultad que he encontrado en el minado de la criptomoneda, ya que como he comentado, usar los monederos y realizar las transacciones no supone ningún obstáculo ya que está pensado

para ser intuitivo para un usuarios medio, sin embargo el minado -actividad principalmente encomendada a programadores e ingenieros- ha requerido de un esfuerzo extra por mi parte para poder finalmente llevarlo a cabo.

Y para terminar, también nos encontramos el problema de la continua actualización y adaptación que en este mundo puede dejar los datos obsoletos en cuestión de días., por lo que es imprescindible mantenerse continuamente informado sobre los incesantes hallazgos en esta materia.

5 Bibliografía

A scalable, interoperable & secure network protocol for the next web. (2021). Polkadot. Recuperado el 5 de Julio de 2021, en: https://bit.ly/2ULIaqp

A. (2019, noviembre 7). Exchange Privado. Más barato, más rápido, más exchange [Imagen] BitcoinHardwareWallet.pro. Recuperado de: Recuperado el 27de mayo del 2021, en: https://bit.ly/2UMrRcX

Academy, B. (2020, 10 noviembre). ¿Qué es un Hard Fork? Bit2Me Academy. Recuperado el 20 de junio del 2021, en: https://bit.ly/3kf2OtU

Academy, B. (2021, 22 febrero). ¿Qué es un token NFT? Bit2Me Academy. Recuperado el 25 de Junio de 2021, en*: https://bit.ly/3AXfH1w*

Academy, B. (2021, 31 mayo). ¿Qué es Cardano (ADA)? Bit2Me Academy. Recuperado el 3 de Julio de 2021, en :*https://bit.ly/3yR0Vrl*

Academy, B. (2021, 25 junio). Bit2Me Academy | Formación de Bitcoin y Criptomonedas. Bit2Me Academy. Recuperado el 19 de Mayo de 2021, en*: https://bit.ly/3hDog4*

Academy, B. (2021, 10 noviembre). ¿Qué es la Cadena de Bloques (Blockchain)? Bit2Me Academy. Recuperado el 24 de Mayo de 2021, en: https://bit.ly/3i3ZYFn

Banco Santander. (2021). Guía para saber qué son las criptomonedas. Recuperado el 27 de Mayo del 2021, en : https://bit.ly/3oNdArr

Barceló, I. [Economipedia]. (2017). Criptomoneda. Recuperado el 20 de Mayo de 2021, en: https://bit.ly/3fiCZ9l

BBC News Mundo. (2021, 10 junio). Bitcoin en El Salvador: qué se sabe sobre la ley que convertirá el país en el laboratorio mundial de la criptomoneda al hacerla de curso legal. BBC News Mundo. Recuperado el 30 de Mayo de 2021, en: https://bbc.in/3kemFcQ

Binance. (2021). Aprenda todo sobre Blockchain y cripto. Recuperado el 20 de Mayo de 2021, en: https://bit.ly/36zLqIq

Bitcoin - Dinero P2P de código abierto. (2009). bitcoin.org. Recuperado el 17 de Mayo de 2021, en: https://bit.ly/3ilbA7h

Cardano is a decentralized public blockchain and cryptocurrency project and is fully open source. (2021). Cardano. Recuperado el 24 de Mayo del 2021, en: https://bit.ly/3AWlMve

Casos de Uso del Blockchain: el Internet de las Cosas (IoT). (2019, 16 abril). BINANCE ACADEMY. Recuperado el 27 de Mayo del 2021, en: https://bit.ly/3AUyoD8

Chamizo, H. (2021, 25 abril). Los proyectos más innovadores detrás de las criptomonedas de moda. Business Insider España. Recuperado el 22 de Mayo del 2021, en: https://bit.ly/3kd3gst

CRIPTOMO - Edición en Español. (2021, 11 enero). CRIPTOMO. https://bit.ly/2TWsvot

Entiende Bitcoin y Ethereum - Explicación técnica a fondo en español sobre Criptomonedas. (2017, 7 septiembre). [Vídeo]. YouTube. Recuperado el 1 de Julio del 2021, en: https://bit.ly/2U4Ar72

Ethereum. (2021a). Las actualizaciones de Eth2. ethereum.org. Recuperado el 27 de Mayo del 2021, en: https://bit.ly/3ee5lAK

Ethereum. (2021). ¿Qué es Ethereum? ethereum.org. Recuperado el 27 de Mayo del 2021, en: https://bit.ly/3AYuuZV

Fernández, C. (2018, 30 abril). Valladolid crea VaCoin para fomentar la tecnología blockchain entre sus ciudadanos. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas. Recuperado el 5 de Julio del 2021, en: https://bit.ly/3hyRCqk

Funciones del Exchange. (2019, 7 octubre). [Imagen]. Recuperado el 1 de Julio del 2021, en: https://bit.ly/2UMrRcX

Galeano, S. (2018, 26 marzo). Así funciona Ripple, la criptomoneda por la que apuestan los bancos. Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce. Recuperado el 2 de Julio del 2021 en: *https://bit.ly/3hyRCqk*

Golem Network. (2021). Golem Network. Recuperado el 7 de Julio del 2021, en: https://bit.ly/36xJ38N

Gil, J. J. (2020, 27 septiembre). *Guía Ethereum, mucho más que una simple criptomoneda.* bitcobie. Recuperado el 29 de Junio del 2021, en: https://bit.ly/36wtEWa

HardWallet. (2019). [Imagen]. Recuperado el 20 de Junio del 2021, en : https://www.walletgenerator.net/?culture=es¤cy=vergecoin

HISTORIA del DINERO | Draw My Life. (2019, 20 febrero). [Vídeo]. YouTube. Recuperado el 10 de Julio del 2021, en: https://bit.ly/3hYd9Ys

Lanzan una criptomoneda que financiará la preservación del medio ambiente. (2021, 20 febrero). Télam - Agencia Nacional de Noticias. Recuperado el 30 de Mayo del 2021, en: https://bit.ly/3hxCNnU

León, O. R. (2021, 27 mayo). *¿Qué es Ethereum 2.0 y qué pasará con la actualización?* Oink Oink. Recopilado el 30 de Mayo del 2021, en: https://bit.ly/3wBOoGO

Maldonado, J. (2020, 15 septiembre). *¿Qué es Polkadot?* Cointelegraph. Recuperado el 4 de Julio del 2021, en : https://bit.ly/3AUAXoK

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260. Recuperado el 15 de Mayo del 2021, en: https://bit.ly/3edgLoo

Opera Browser. (2021). Opera. Recuperado el 1 de Julio del 2021, en: https://bit.ly/3kd6A7d

Pastor, J. (2018, 17 mayo). *Así es Monero, la criptomoneda preferida de los cibercriminales por dos razones: anonimato y privacidad*. Xataka. Recuperado el 29 de Mayo del 2021, en: https://bit.ly/3yXYe7D

Pastor, J. (2020, 6 mayo). *Qué es el «bitcoin halving» y por qué está provocando que el valor de bitcoin crezca un 18% en las últimas 24.* Xataka. Recuperado el 20 de Mayo del 2021, en: https://bit.ly/3yTOs6a

¿Qué es Ethereum y cómo funciona? (2021). IG. Recuperado el 21 de Mayo del 2021: https://bit.ly/3kd5s3b

*¿*Qué *es una wallet o monedero de criptomonedas?* (2021, 8 febrero). bit2me ACADEMY. Recuperado el 15 de Mayo del 2021, en: https://bit.ly/3xG0Syk

15 aplicaciones de la tecnología blockchain más allá de bitcoin | Fintech. (2016, 13 octubre). FinTech. Recuperado el 18 de Mayo del 2021, en: https://bit.ly/2U4CKqI

15 ventajas y 5 desventajas del bitcoin. (2014, 15 enero). 3Cero. Recuperado el 16 de Mayo del 2021, en: https://bit.ly/3wBYAPB

R. (2019, 17 septiembre). :es: Fases del desarrollo de Cardano. Cardano Forum. Recuperado el 27 de Mayo del 2021, en: https://bit.ly/3kd674F

Sephton, C. (2021). Precio, gráficos, capitalización de mercado de Ethereum (ETH). CoinMarketCap. Recuperado el 17 de Mayo del 2021, en: https://bit.ly/3ewanJd

Tejedo, E. (2020, 7 agosto). Bitcoin: pros y contras de la moneda de internet. Foxize. Recuperado el 26 de Mayo del 2021, en: *https://bit.ly/3kcSna9*

Uniswap. (2021). Home. Recuperado el 2 de Julio del 2021, en: https://bit.ly/2Tby1Dg

Varshney, A. (2021). *Precio, gráficos, capitalización de mercado de Cardano (ADA)*. CoinMarketCap. Recuperado el 1 de Julio del 2021, en: https://bit.ly/3yXhjqt

6 Anexos

6.1 Glosario

Bitcoin (con B mayúscula): se utiliza para describir el concepto de bitcoin, la red y el protocolo que mantienen su blockchain y su criptomoneda.

bitcoin (con b minúscula): se refiere a la unidad de la criptomoneda basada en la red homónima, pudiendo ser usada en singular y en plural (bitcoin y bitcoins).

Bloque génesis: denominación que se le da al primer bloque creado y verificado en una blockchain. Este bloque marca el nacimiento de cada criptomoneda. El primero de su tipo fue el bloque génesis de Bitcoin, creado en enero de 2009 por Satoshi Nakamoto.

Cartera, billetera o monedero (Wallet): software que gestiona direcciones (cuentas) y llaves (contraseñas) de blockchains para consultar, enviar y recibir criptoactivos. Hay carteras con aplicaciones para móviles, de escritorio, en cajeros automáticos o casas de cambio, además de hardware

Casa de Cambio (Exchange): es el lugar físico o digital donde se realizan operaciones de cambio de moneda. Está organizado para intercambiar monedas entre un comprador y un vendedor, que puede ser la propia casa de cambio, y se cobra una comisión por su compra y por su venta. El precio de la divisa o criptomoneda se congela durante el tiempo de la transacción. LocalBitcoins es un ejemplo de casa de cambio.

Corretaje (Trading): son las gestiones que realiza el corredor para materializar su encomienda, la compra y venta de algo por cuenta del mandante. En el ámbito blockchain, trading alude a la compraventa especializada de criptomonedas con miras a conseguir ganancias.

Criptografía: se trata de un conjunto de técnicas de cifrado de información que funcionan para proteger data sensible. En el ámbito informático, estas técnicas se construyen con matemática compleja (como los algoritmos) y se usan para proteger datos y comunicaciones. Las criptomonedas y las blockchain están construidas con criptografía avanzada.

Criptoactivo: token o ficha construida a base de criptografía, que es emitida y comercializada en una red blockchain. El término se acuña y populariza ante la expansión de las rondas de financiamiento y venta inicial de monedas (ICO) y el establecimiento de las nuevas dinámicas financieras en las casas de bolsa.

Criptomoneda: moneda basada exclusivamente en la criptografía. A diferencia de las monedas emitidas por gobiernos y bancos centrales, se genera con la resolución de problemas matemáticos basados en criptografía. Su valor, no obstante, está sujeto a variación de precios, dependiendo de la oferta y demanda en los mercados.

DApps: Acrónimo de aplicaciones descentralizadas, estas son programas de ejecución distribuida en múltiples dispositivos que (generalmente) se basan en Smart contracts para su funcionamiento.

DeFi: Acrónimo de: *Decentralized Finance* o finanzas descentralizadas, son aquellos ecosistemas financieros abiertos

Descentralización: es el proceso de distribuir o dividir ciertas funciones, poderes, personas o cosas más allá de una autoridad central. Dentro del mundo de las criptomonedas, implica que un sistema no es manejado por una única parte, sino que sus nodos —ordenadores— y desarrolladores están distribuidos entre distintas partes y la toma de decisiones se realiza en conjunto.

Dinero Fíat (Fiat): dinero emitido por una entidad autorizada por mandato de Ley, usualmente el Banco Central del país. En inglés se ha popularizado la palabra 'fiat' como sinónimo de dinero fíat.

Halving/Halvening: término referente a la reducción por la mitad de la recompensa que reciben los mineros por confirmar los bloques de transacciones únicas en una criptomoneda. En Bitcoin ocurre cada 210.000 bloques minados, es decir, aproximadamente cada 4 años.

Hash o hash criptográfico: es un algoritmo que cuenta con ciertas propiedades útiles para el cifrado de datos, esto es, proteger contenidos mediante el uso de claves. Al aplicarla, se toma un mensaje de cualquier tamaño, se cifra, y se consigue a cambio una cadena alfanumérica única de longitud fija (llamada *digest* o simplemente hash), sin importar el tamaño del mensaje original.

Hashrate (Tasa o velocidad de hash / poder de procesamiento o cómputo): esta tasa mide la potencia de procesamiento en una criptomoneda, o, dicho de otra forma, es el número de operaciones de hash realizadas en cierta cantidad de tiempo. Por ejemplo, cuando una red alcanza un hash rate de 6TH/s significa que puede realizar hasta 6 billones de operaciones por segundo.

Initial coin offer (ICO): Son los lanzamientos de proyectos de criptomoneda, su objetivo es la financiación del proyecto, el concepto es similar al que vemos en el Crowdfunding.

IoT: *Internet of things* o internet de las cosas hace referencia a las interconexiones realizadas entre diferentes aparatos y sensores que se comunican entre si a través de internet.

Minería (de criptomonedas): es el proceso mediante el cual se resuelven complejos problemas matemáticos para validar transacciones en una cadena de bloques y emitir nuevas monedas.

Nexus mutual

Nodo: en redes de computadoras, se refiere a un ordenador o servidor conectado a la red, que es capaz de transmitir información a otros. Una blockchain descentralizada está compuesta por múltiples nodos.

Nonce: Es el código que se añade al final de cada bloque para que el *Hash* reúna los requisitos designados en la prueba de trabajo.

Pool de minería: es la agrupación de dos o más mineros que juntan su poder de cómputo para elevar las posibilidades de resolver un bloque y obtener una recompensa más constante. En los pools de minería, la recompensa se divide internamente en función de la cantidad de hashes aportados por cada uno de sus integrantes.

PoW: Acrónimo de *Proof of work* o prueba de trabajo

Roadmap (Mapa/Hoja de Ruta): se trata del plan —usualmente reflejado en un documento— que una compañía o proyecto describe para incluir todo lo que quiere lograrse a futuro. Se estructura en metas acompañadas de fechas específicas.

Satoshi: es la penúltima subdivisión más pequeña que puede obtener un bitcoin, a saber: 0.00000001 BTC.

Smart Contracts: Contratos auto ejecutables, de plena validez legal y contenidos en un código mediante comandos por lo que al reunir ciertas condiciones se ejecutaran unas acciones previamente establecidas.

Stable coin: Son aquellas monedas cuyo valor se encuentra asociado al de otra moneda o activo (de relativa estabilidad) que se emplean para reducir el riesgo a la hora de operar y realizar *swaps* con otras criptomonedas.

Staking: se puede traducir como “apostar”, pero se refiere al proceso mediante el cual un usuario adquiere y bloquea cierta cantidad de tokens en una red PoS para validar las transacciones y recibir recompensas.

Swap: Consiste en intercambiar una criptomoneda por otra a través de un intermediario.

Token: en el mundo de las criptomonedas, es una moneda digital construida con criptografía que depende de la blockchain de otra moneda para existir, así que se rige por sus reglas. Son como monedas creadas dentro del sistema de otra moneda y es usual que se diseñen con distintas aplicaciones integradas. El término también puede aludir a cualquier criptomoneda en general.

Whitepaper: Es un documento que recoge información sobre un tema o una idea que se quiere exponer en profundidad.

6.2 Acrónimos criptomonedas.

BTC: Bitcoin

BTH: Bitcoin Cash

XRM: Monero

ETH: Ethereum

IOTA: IOTA

BLK: Blackcoin

DASH: Dash

ADA: Cardano

HRM: Hermes