TRABAJO DE FIN DE GRADO

TECNOLOGÍA BLOCKCHAIN: ORIGEN, FUNCIONAMIENTO Y USOS

BLOCKCHAIN TECHNOLOGY: ORIGIN, FUNCTIONING AND USES

Autor

Claudia Marín Pérez

Director

Luis Ferruz Agudo

Facultad de Economía y Empresa, Universidad de Zaragoza

2021-2022

Autor del trabajo: Claudia Marín Pérez

Director del trabajo: Luis Ferruz Agudo

Título del trabajo: Tecnología Blockchain: Origen, funcionamiento y usos

Blockchain Tecnhology: origin, funtioning and uses

Titulación: Programa Conjunto de Derecho y Administración y Dirección de Empresas

Resumen (200 palabras)

En la actualidad la tecnología es nuestro mejor aliado y gracias a su evolución surge por primera vez en 2008 la primera aplicación de la tecnología blockchain. Esta tecnología supone una disrupción en el sistema tradicional, abriendo las puertas a realizar transacciones sin intermediarios de forma segura, rápida y a un menor coste. La principal difusión práctica de conocimiento público viene de la mano del concepto criptomonedas, pero esta va mucho más allá. En este trabajo se analiza el funcionamiento de esta tecnología desde su origen explicando dos conceptos clave: DLT y encriptación, así como las principales características de la misma. Además, se estudian los usos como activo para mantener valor, para brindar una utilidad y como token respaldados por bienes físicos; así como otras formas de monetización relevantes.

Abstract

Nowadays, technology is our best ally and thanks to its evolution, the first application of blockchain technology appeared for the first time in 2008. This technology represents a disruption in the traditional system, opening the doors to carry out transactions without intermediaries, securely, quickly and at a lower cost. Its main utility comes from the concept of cryptocurrencies, but it goes much further. This paper analyses the functioning of this technology from its origin, explaining two key concepts: DLT and encryption, as well as its main characteristics. In addition, the uses as an asset to hold value, to provide a utility and as a token backed by physical goods are studied, as well as other relevant forms of monetisation.

ÍNDICE

ILUSTRACIONES

Abreviaturas

BTC. Bitcoin

CBDC. Monedas digitales emitidas por bancos centrales

DLT. Distributed *Ledger* Tecnhology

ETH. Ethereum

FMI. Fondo Monetario Internacional

ICO. Initial Coin Offering

IRPF. Impuesto sobre la Renta de las Personas Físicas

NFT. Non Fungible Tokens

PoW. Proof of Work

PoS. Proof of Stake

P2P. Peer-to-Peer

I. INTRODUCCIÓN

1. OBJETO Y OBJETIVO DEL TRABAJO

Vivimos en un mundo de constante cambio y evolución, donde la tecnología es nuestro mejor aliado. A partir de la creación de Internet, las bases de datos han sido un sistema clave y una necesidad en la sociedad. Esto ha llevado al nacimiento de una tecnología descentralizada denominada Blockchain o cadena de bloques. Hasta ahora las transacciones que realizábamos tradicionalmente tenían un intermediario que las verificaba y controlaba, mientras que gracias a los nuevos usos de esta tecnología estos procesos pueden democratizarse. Uno de los proyectos más conocidos de la Blockchain es Bitcoin, pero hay muchísimas más criptomonedas, así como otros muchos usos a partir de la aplicación de esta tecnología que evoluciona de forma vertiginosa. Como decía Marc Kenigsberg: "El Blockchain es la tecnología. Las criptomonedas son simplemente la primera manifestación de su potencial"[1].

El objeto de este trabajo es analizar el origen y explicar el funcionamiento de esta tecnología, indicando las características básicas y categorizando los distintos proyectos de las criptomonedas y otras aplicaciones más allá de estas. En definitiva, se analizan distintas formas de monetizar la tecnología DLT (Distributed Ledger Tecnhology), referida a libro contable o almacenamiento de datos distribuido.

Todo ello con el objetivo de realizar un compendio estructurado de información actualizada sobre el tema objeto tratado desde una perspectiva financiera y jurídica con vistas a tener un informe de Consultoría / Asesoría eminentemente práctico, operativo y profesional sin menoscabo de la rigurosidad universitaria y académica.

2. JUSTIFICACIÓN DE LA ELECCIÓN DEL TEMA

La elección del tema objeto de estudio responde principalmente a una motivación personal dado mi interés por la tecnología y sus aplicaciones en nuestra sociedad. Tras el boom de las criptomonedas, concretamente desde la aparición de Bitcoin como uno de los proyectos a los que se aplica la tecnología Blockchain, me he visto intrigada por su evolución y sus distintas aplicaciones. Este nuevo fenómeno ha revolucionado el

[1] SOLERA, S. (2021). *Blockchain: qué es, cómo funciona y los usos más comunes*. OCCAM. [consultado 10/11/2021]. Disponible en: https://www.occamagenciadigital.com/blog/Blockchain-que-es-como-funciona

sistema actual sobre todo a nivel económico, por lo que considero relevante hacer un análisis de la situación actual, así como de las aplicaciones que se le ha dado dejando de lado ciertos sistemas tradicionales.

Es esencial tener en cuenta que al hablar de criptomonedas no nos referimos a otra cosa distinta del dinero digital, concepto con el que ya estábamos familiarizados con cuentas bancarias electrónicas y las tarjetas de crédito que utilizamos a diario. Lo realmente innovador es la utilidad de estas como sistema de pago, ya que por primera vez nos permite intercambiar dinero digitalmente sin intermediario y bajo cierto anonimato.

Sin embargo, a pesar de las virtudes de las monedas digitales privadas, no se puede olvidar los riesgos que conllevan. En primer lugar, tan sólo el Gobierno del Salvador actualmente respalda su uso, por lo que todavía no se puede decir que exista una confianza sobre estas como medio de pago efectivo, ya que no está clara la evolución desde una perspectiva social en el sentido de aceptación. En segundo lugar, la elevada volatilidad que depende de las expectativas de confianza sobre el resto de las personas aportándole mayor o menor valor, lo que provoca que su precio no sea estable y que no sean de utilidad como valor de reserva según indicaba Jerome Powell, presidente de la Reserva Federal de los Estados Unidos[2]. El papel de los bancos centrales es adecuar la oferta de sus dividas a las condiciones económicas, pero en este caso ¿en quién recae esa responsabilidad? Finalmente, se debe tener en cuenta que las transacciones en la red son irreversibles, además, del riesgo regulatorio que existe ante la falta de normativa aplicable, provocando caídas de valor elevadas ante distintos pronunciamientos. Todo ello, sin olvidar el elevado consumo de energía que conlleva implicaciones medio ambientales.

Mi formación me ha permitido adquirir competencias en el ámbito económico y legal, lo que me hizo plantear este tema desde ambas perspectivas. A través de este trabajo pretendo acercar esta tecnología para una mejor comprensión de esta, no sólo explicando su origen y funcionamiento, sino las múltiples aplicaciones que tiene, suponiendo una innovación disruptiva en el sistema económico tradicional.

3. METODOLOGÍA

[2] BELINCHÓN, F. (2021, 1 abril). Riesgos de las divisas virtuales para los particulares. EL PAÍS, Cinco Días [consultado 13/02/2022]. Disponible en: https://cincodias.elpais.com/cincodias/2021/04/01/mercados/1617278607_020694.html

Para alcanzar los objetivos que se plantean, se ha utilizado una metodología de tipo descriptivo, literario e institucional en contexto financiero y jurídico. A continuación, se indica la estructura del trabajo:

En primer lugar, se analiza la tecnología DLT en sí misma haciendo una recapitulación de su origen desde el surgimiento de Internet. Se plantea la necesidad de crear sistemas de almacenamiento eficaces que hasta día de hoy estaban centralizados. Se indican dos ejemplos clave para entender esta tecnología: Netflix y BitTorrent.

Seguidamente se explican los tipos de encriptación y el proceso de encriptación que se sigue hasta conseguir el objetivo deseado, parte esencial para entender la cadena de bloques. Se indican tres elementos clave de este proceso y la implicación en la Blockchain.

En segundo lugar, se hace alusión a la tecnología Blockchain y sus principales características que la hacen única. Para una mejor comprensión hacemos hincapié en las criptomonedas como la aplicación principal de esta tecnología y se indican los tipos de usos que hay detrás de ellas: como criptomonedas de valor, de utilidad y de token[3].

En tercer lugar, se desarrolla el concepto de Wallet y Exchanges como medios y plataformas clave detrás de las criptomonedas que nos permiten comercializar con ellas dentro de una red Blockchain.

Finalmente, se indican otras formas de monetizar la Blockchain que considero pueden ser relevantes para posibles retos futuros en la economía, más allá de la especulación con criptomonedas. Se hace referencia a la participación en el minado, en los protocolos de consenso, las finanzas descentralizadas, la inversión en empresas que utilizan protocolos basados en Blockchain, así como los creadores de contenido a través de NFTs, entre otros.

[3] ZAVALA, A., (2018). Blockchain: qué es un token y los usos que puede llegar a tener. EXPANSIVE [consultado 24/12/2021]. Disponible en: https://blog.expansive.mx/2018/03/08/Blockchain-que-es-un-token-y-los-usos-que-puede-llegar-a-tener/

II. DLT

Internet nace a partir de diversos avances tras su origen en 1947 y hoy en día es una herramienta fundamental para muchos de nosotros que ha cambiado nuestra forma de actuar, de comunicarnos y de trabajar. En poco tiempo se llevaron a cabo grandes avances. En EE. UU. se crea la Advanced Research Projects Agency (ARPA) como respuesta a los desafíos tecnológicos.

Profundos cambios económicos y socioculturales, mejora en las comunicaciones, expansión del conocimiento e incluso cambios en la conducta de las personas han venido de la mano de Internet. Actualmente, la vida sin internet es casi inconcebible a todos los niveles, a pesar de que en un primer momento estaba basada en una tecnología poco accesible y difícil de utilizar que requería el conocimiento de expertos. Con su evolución se fue volviendo más accesible, se desarrollaron protocolos estandarizados y surgieron nuevas aplicaciones con interfaces sencillas. Hoy en día todos tenemos un teléfono móvil con conexión a internet, y sabemos acceder a cualquier tipo de información online sin la necesidad de entender el funcionamiento interno del teléfono ni de las señales que nos brindan el internet.

Este desarrollo de nuevas tecnologías hace que nos replanteemos la llamada cuarta revolución industrial, en la que se busca la eficiencia a través de un uso más consciente y cuidadoso de los recursos y la propiedad.

Dentro de este contexto, las bases de datos se han convertido en una herramienta clave, surgiendo la necesidad de crear sistemas de almacenamiento eficaces. Hasta día de hoy, dichos sistemas estaban centralizados y tenían grandes gastos de mantenimiento. Por ello, se plantean nuevas formas de almacenar la información como es la tecnología "DLT (*Distributed Ledger Technology*)"[4].

Atendiendo a su origen, en ocasiones esta tecnología se confunde con Blockchain. Sin embargo, a pesar de que podamos afirmar que Blockchain es una DLT, tan sólo es una implementación de esta.

[4] West, P. (2018, 19 febrero). *Is distributed ledger technology the answer? Open Innovation Team*. OPENINNOVATION [consultado 17/11/2021]. Disponible en: https://openinnovation.blog.gov.uk/2018/02/19/is-distributed-ledger-technology-the-answer/

Ante la necesidad de almacenar gran cantidad de datos nacen distintas ideas enfocadas en optimizar tanto los costes como los protocolos a través los cuales esa información es modificada. La mejor idea viene a llamarse Blockchain.

De forma sencilla, podríamos explicar el funcionamiento de la Blockchain como un proceso que permite a los nodos en una red proponer, validar y registran cambios de estado en un libro mayor sincronizado/distribuido a través de dichos nodos. Es decir, cada nodo participante cuenta con una réplica de este libro, evitando así que los datos se vean comprometidos en caso de fallo en algún nodo.

El continuo intercambio y actualización de registros de igual a igual hace que el proceso sea más rápido, eficaz y económico gracias al uso que hacen estas redes de los protocolos "peer-to-peer" (P2P). Gracias a los nodos, ordenadores o unidades de cómputo básicas que operan con el mismo software, se anotan en esta plataforma todas las transacciones que ocurren en el orden exacto. En el momento en el que se produzca algún cambio en una de las réplicas de ese registro o ledger, todas se actualizarán mediante consenso. Esto permite que las transacciones no necesiten permiso de un ente central, sino que el papel de este tercero lo hace la red P2P, validando y verificando todo lo que ocurre. De esta forma surge un sistema "democratizado", que otorga seguridad y confianza a los registros que se añaden en la red, que aumenta cuanto mayor sea el número de nodos, evitando que uno o la suma de unos pocos puedan tomar decisiones contrarias al resto.

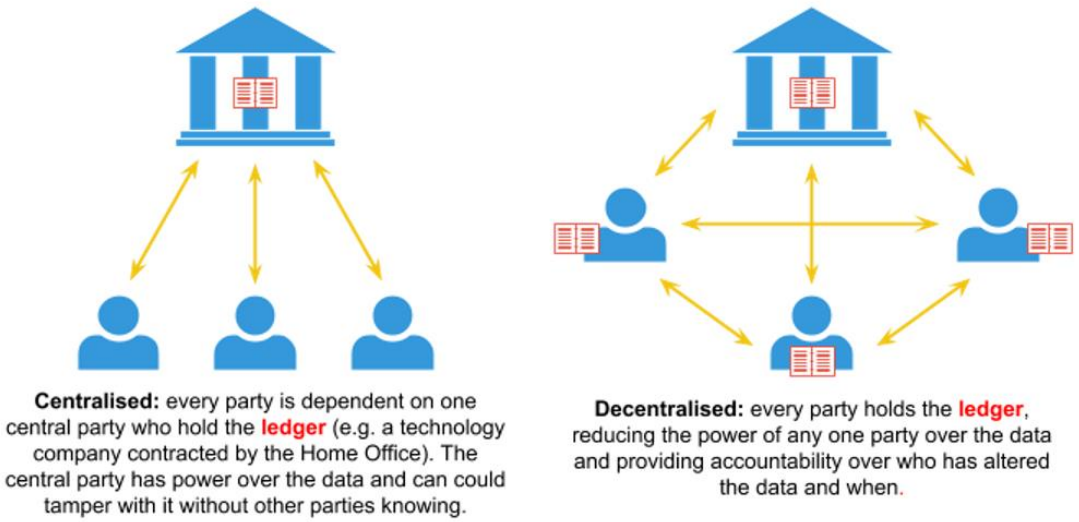

Ilustración 1- Comparativa entre el funcionamiento de un libro centralizado y un libro distribuido

Fuente: Openinnovation.blog.gov.uk

En función de cómo sea el acceso de participantes a la red, suelen distinguirse las redes públicas de las privadas. Las plataformas públicas y de código abierto son aquellas en las que puede participar cualquiera, mientras que las privadas requieren autorización previa. Las normas y el funcionamiento de cada una de ellas en particular quedarán recogidas en su código. Esto aparece representado gráficamente en la figura 2 que se muestra a continuación.

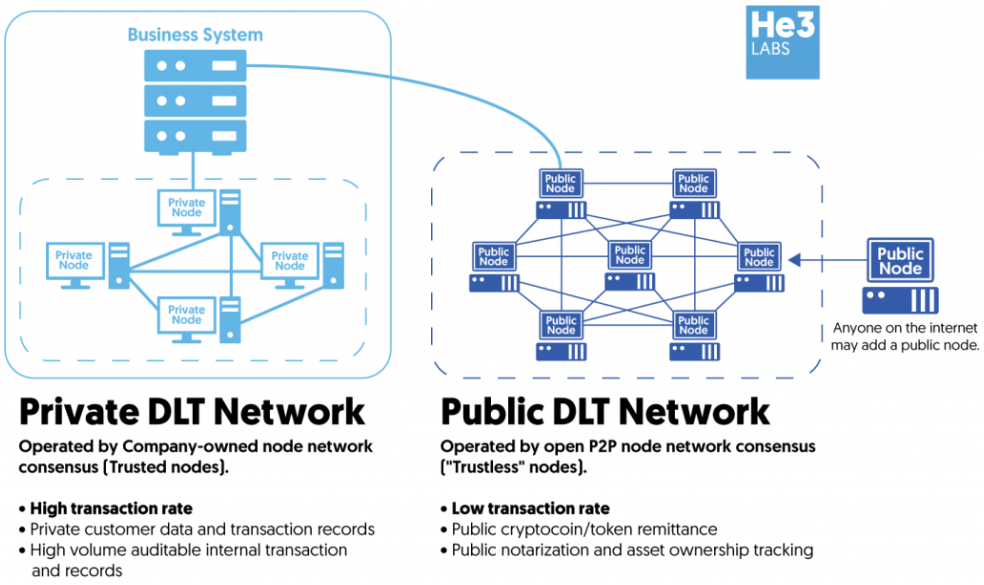

Ilustración 2- Comparativa entre las plataformas DLT privadas y públicas

Fuente: He3labs

Esta tecnología está presente en muchos aspectos de nuestras vidas, y sin irnos muy lejos, podemos hacer referencia a ***Netflix***. Esta plataforma de contenidos audiovisuales en streaming te permite ver películas y series a la carta gracias a un servicio por suscripción. Pero ¿de dónde sale todo el contenido que vemos en Netflix? Amazon Web Services (AWS) y Open Connect son la respuesta. Ambas son nubes de almacenamiento y gestión de contenido, redes de distribución, que trabajan de forma conjunta[5]. Almacenan vídeos y cuando queremos reproducirlos, la retransmisión se realiza desde esas redes a nuestro dispositivo. Sin embargo, al tratarse de una red centralizada en caso de haber algún problema con AWS u Open Connect, el servicio puede caer.

Siguiendo otro ejemplo, de una plataforma de streaming que usa una tecnología más próxima a Blockchain, encontramos a ***BitTorrent***.

[5] Hoff, T. (2018, 10 febrero). *La compleja infraestructura detrás de Netflix: ¿qué pasa cuando le das al «play»?* XATAKA. [consultado 28/11/2021]. Disponible en: https://www.xataka.com/streaming/la-compleja-infraestructura-detras-de-netflix-que-pasa-cuando-le-das-al-play

Este es un protocolo de intercambio de datos de forma descentralizada. Este sistema siempre ha sido popular respecto al intercambio de archivos de todo tipo, y aunque la descarga directa le quitó protagonismo durante unos años, ahora vuelve a ser un protocolo muy utilizado. La información, o en este caso la película, se encuentra almacenada en diferentes ordenadores distribuidos por el mundo. Cuando un usuario quiere ver un vídeo, la red busca el ordenador más cercano que tenga el vídeo y el streaming se produce desde ese servidor, proporcionando así rapidez y eficacia[6]. Utilizando por tanto lo explicado anteriormente, el protocolo P2P, en el que los clientes se conectan directamente entre ellos sin pasar por un servidor central. Tú quieres bajar un archivo, y debes abrir el archivo específico .torrent, que sirve como mapa para llegar hasta el archivo que quieres bajar.

En resumen, las plataformas DLT son fundamentalmente el resultado de combinar tecnologías como las redes P2P, los algoritmos de consenso, concretamente lo que se denomina proof of work que explicaremos más adelante; y la criptografía, proceso que desarrollamos en el apartado siguiente. La propia naturaleza de esta tecnología global, pública e incensurable hace que toda la información incorporada en ella sea inmune a un hackeo.

[6] Fernández, Y. (2021, 8 febrero). *BitTorrent: qué es y cómo funcionan los torrents.* XATAKA. [consultado 01/12/2021]. Disponible en: https://www.xataka.com/basics/bittorrent-que-como-funcionan-torrents

III. **CRIPTOGRAFÍA:** ¿Cómo funciona el proceso de encriptación?

La RAE[7] define la criptografía como el arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que tenga la clave. En la actualidad, este sistema ha evolucionado considerablemente al ser aplicado a la informática con la finalidad de salvaguardar la seguridad de las comunicaciones e informaciones que se comparten a través de Internet.

Existen dos tipos de criptografía, simétrica y asimétrica[8]. La primera de ella atiende al método en el que conociendo el método de encriptación cualquier persona puede encriptar y descifrar mensajes, mientras que la segunda, la criptografía asimétrica hace referencia a un sistema que optimiza la seguridad en el envió de información de una persona a otra, de esta manera una persona dispone de dos claves, la llamada clave pública y la clave privada.

Ambas claves pertenecen a la misma persona y si una persona emite un mensaje a un destinatario, este debe cifrarlo con la clave publica de la persona que debe recibir la información, ya que solamente el poseedor de la clave privada que funciona de llave podrá recibir el mensaje.

Cualquier persona puede cifrar un mensaje si conoce la clave publica, pero únicamente el poseedor de la llave privada puede descifrarlo.

La clave pública se usa para recibir transacciones, y la clave privada para firmarlas y gastar fondos asociados a una cuenta si los hubiera. El proceso de encriptación está basado en funciones matemáticas, creando secretos digitales y firmas infalsificables. De hecho, existe una relación matemática entre las claves públicas y privadas que permiten que la clave privada se use para generar firmas y estas sean validadas contra la clave pública sin desvelar la privada.

Es este segundo tipo de criptografía en la que se centra el trabajo.

---

[7] Real Academia Española (2021). "Criptografía". En: *Diccionario de la Real Academia Español*. [consultado 11/11/2021]. Disponible en: https://dle.rae.es/criptograf%C3%ADa

[8] Blockchain 101. (2020, 11 enero). *The cryptography used in Blockchain*. APRENDE BLOCKCHAIN. [consultado 17/12/2021]. Disponible en: https://aprendeBlockchain.wordpress.com/Blockchain-101-ii/

Blockchain 101. (2018, 18 febrero). *Conceptos de seguridad y criptografía en Blockchain*. APRENDE BLOCKCHAIN. [consultado 18/12/2021]. Disponible en: https://aprendeBlockchain.wordpress.com/fundamentos-tecnicos-de-Blockchain/fundamentos-basicos-de-criptografia-en-Blockchain/

Sea como sea, parea entender de manera sencilla la criptografía únicamente debemos tener en cuenta 3 cosas:

- Input
- Proceso de encriptación
- Output

Siendo la primera el mensaje que queremos cifrar, la segunda es el protocolo a través del cual la información es encriptada y la tercera es el resultado o el mensaje encriptado. Para conceptualizarlo sirve de ejemplo el sistema de cifrado César, también conocido como cifrado por desplazamiento[9]. Se trata de una de las técnicas de cifrado más simples en el que se sustituye cada letra del texto por otra letra que se encuentre un número fijo de posiciones más adelante en el alfabeto.

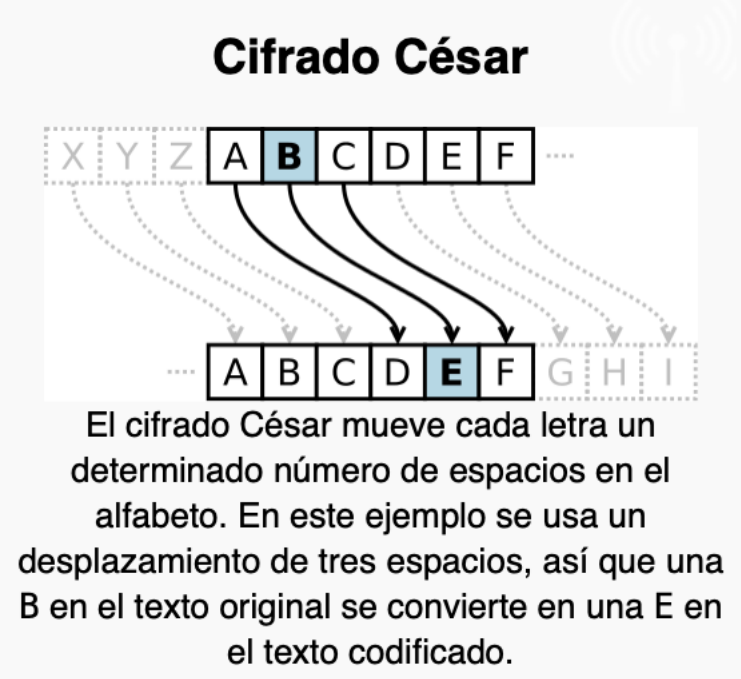

Ilustración 3- Cifrado César

Fuente: IBM Community- Z Security

De esta manera un ejemplo de input seria "Hola" y con un proceso de encriptación Cesar +2 el output resultante seria "Jqtc".

Este es uno de los ejemplos más sencillos de encriptación simétrica.

[9] SUBHASISH, S. (2020, 4 julio). Know about the Caesar Cipher, one of the earliest known and simplest ciphers. IBM Community- Z Security [consultado 17/11/2021]. Disponible en: https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/04/caesar-cipher

Debido a los ordenadores y a su gran capacidad computacional dentro de la Blockchain la encriptación tiene otra función principal, y es que el verdadero objetivo de la encriptación reside en su participación en lo que conocemos como Proof Of Work (POW).

Los nodos, son aquellos ordenadores que mantienen una copia de la Blockchain y su función no reside únicamente en verificar y votar que información es almacenada, sino que también son los encargados de encontrar la forma en la que esta información es almacenada.

Habiendo visto que tipos de encriptación existen y los principios básicos de su funcionamiento, cabe destacar otra de sus cualidades, y es que cuando hablamos de encriptación asimétrica es relativamente sencillo encriptar algo, únicamente necesitamos el input, el proceso de encriptación, y obtenemos el output. Sin embargo, las cosas se complican cuando queremos un output que cumpla ciertos requisitos (que acabe en 9, que tenga 5 ceros…) y es que, en este tipo de encriptación unidireccional si queremos obtener un output concreto la única forma es a través de prueba y error, dejar que el ordenador pruebe millones de inputs diferentes hasta dar con el output deseado.

El primer momento en el que se necesitó de la capacidad de hacer trabajar a un ordenador más tiempo para lograr un mismo objetivo se remonta a la aparición del email y de los emails "spam". Tras el surgimiento del email no fue difícil encontrar la tecnología para poder mandar millones de emails en una duración muy breve de tiempo, sirviendo esto a las empresas como método de marketing gratuito.

Los efectos de los conocidos como "mensajes basura" y su desagrado al público en general contribuyeron a que se desarrollara uno de los primeros protocolos de "Proof of Work" que se conocen. De esta manera cada email que mandamos para ser enviado requiere de un problema de cálculo, lo cual supone décimas de segundo para un ordenador cualquiera, pero en el caso de que ese ordenador enviase millones esto le supondría un aumento en el tiempo de envió y su consecuente gasto de electricidad.

De esa manera todos los nodos de una red Blockchain deben verificar la información y competir entre ellos por encontrar el output deseado, demostrando que han trabajado para lograrlo, de ahí su nombre "Prueba de Trabajo" o Proof of Work", siendo el que lo encuentre recompensado.

Al output de ese proceso de encriptación se le conoce como función hash, estas funciones hash son el sello de seguridad de una información almacenada, y es que como se ha mencionado previamente, un output especifico solo se obtiene mediante prueba y error siendo imposible lograr el mismo hash si existe la menor modificación en la información almacenada.

Veamos pues de que está compuesto el input, es decir, de que se compone cada bloque.

Por un lado, encontramos la información, las diferentes transacciones realizadas en el período, habiendo sido esta ya descompuesta en diferente funciones hash según la conocida Raíz de Merkle[10]. Por otro lado, en cada bloque se encuentra el hash (output) del bloque anterior, conectando de esta manera la cadena asegurándonos así de que, si alguien cambia la información de un bloque, su hash cambiará y por tanto hará lo propio el bloque siguiente, y el siguiente y así sucesivamente hasta ver que se ha creado una Blockchain totalmente nueva y que al no ser la misma que la almacenada por el resto de los nodos, no sirve para nada. Y, por último, cada bloque cuenta con un "Nonce"[11] es esa la variable que se va modificando millones de veces hasta hallar el hash correcto.

[10] Raiz de Merkle hace referencia a «una estructura que relaciona todas las transacciones y las agrupa entre pares para obtener un Root Hash o "dirección raíz". Este Root Hash, está relacionado con todos los hashes del árbol. Verificar todas las transacciones de una red sería algo extremadamente lento e ineficiente. Por esta razón, se implementó este sistema. Ya que, si un hash es cambiado, cambiarían todos los demás hasta llegar a la raíz (root hash). Esto invalidará la autenticidad de la información de todo el árbol. Es precisamente esta función, la que permite a los árboles Merkels otorgar el alto nivel de seguridad que los caracteriza.» Academy, B. (2022, 7 enero). *¿Qué es un Árbol Merkle?*. BIT2ME ACADEMY. [consultado 9/01/2022]. Disponible en: https://academy.bit2me.com/que-es-un-arbol-merkle/#:%7E:text=Un%20%C3%A1rbol%20Merkle%20es%20una,todos%20los%20hash%20del%20%C3%A1rbol.&text=Ya%20que%2C%20si%20un%20hash,la%20ra%C3%ADz%20(root%20hash).

[11] CoinTelegraph. (2020, 22 abril). *¿Qué es el nonce? Un número vital en Bitcoin. Investing.com* Español. https://es.investing.com/news/cryptocurrency-news/que-es-el-nonce-un-numero-vital-en-Bitcoin-1991973

IV. FUNCIONAMIENTO DEL BLOCKCHAIN

Antes de empezar a explicar cómo funciona la Blockchain debemos asegurar que quedan claro los diferente elementos y conceptos necesarios para su funcionamiento.

El nombre de Blockchain o cadena de bloques representa la manera en la que almacena la información, así como los libros tienen capítulos, este "libro mayor" tiene bloques. Estos bloques suelen almacenar información de transacciones con un token, que puede tener valor en algún tipo de mercado o no, las transacciones se van añadiendo a la cadena de manera constante por lo que el orden es importante, es por ello que cuando se escribe un bloque este se encripta para crear un hash y se escribe ese hash en el bloque siguiente, de ahí que sea una cadena.

La Blockchain es un libro mayor en el que se almacenan por orden cronológico todas las transacciones de una moneda o token, los usuarios únicamente necesitan un número de cuenta dentro de esa cadena para recibir tokens en su cuenta y poder enviarlos luego.

Los intervinientes dentro de las cadenas son los usuarios, aquellos que dan valor al token, según su oferta y demanda, y los nodos, aquellos que almacenan toda la información de la cadena, que verifican que cuando hay una transacción, la cuenta exista, tenga fondos… y que compiten entre ellos para encontrar el hash para ser recompensados con la creación de nuevos tokens.

Para ponerse en perspectiva, Bitcoin escribe un bloque cada 10 minutos y al minero (Nodo que encuentra el hash) se le recompensan con 6,25 Bitcoins (2022) que a precio de mercado el cual ronda los 37.000€, cada 10 minutos el Nodo ganador recibe en su cuenta 6,25 BTC por valor a día de hoy de unos 230.000€.

Almacenar información nunca había sido tan rentable, pero hay que entender los motivos y ver como apareció esta tecnología.

Las carencias del sistema monetario, la falta de privacidad, la centralización y el comienzo del auge de la criptografía, llevaron a que diferentes desarrolladores llamados ciberpunk comenzaran a llevar a cabo proyectos y sistemas basados en criptografías que permitiesen pagos sin intermediarios y asegurasen la privacidad tanto del receptor como del emisor. Esta corriente ideológica perduro durante la primera década del siglo XXI y fue lo que llevo a que diferentes proyectos naciesen con el fin de descentralizar los pagos electrónicos y eliminar el uso de monedas fiduciarias basadas en deuda e inflación. Muchas de ellas fracasaron, ya que se basaban en la confianza y seguridad de

un tercero, hasta que llego Bitcoin y, por tanto, la mejor implementación hasta la fecha de la tecnología Blockchain.

La primera vez que se supo algo de este proyecto fue a final de 2008, cuando un usuario bajo el pseudónimo de "Satoshi Nakamoto" publico sobre su trabajo en un nuevo sistema de dinero electrónico completamente **P2P**, sin un tercero[12]. Esta criptomoneda funciona gracias a la tecnología de Blockchain, utilizando un sistema de encriptación mediante **funciones hash,** lo que le otorga una gran seguridad y anonimato.

La tecnología Blockchain es una de las más prometedoras en los próximos años, pudiendo ser aplicada en múltiples ámbitos y sectores gracias a las posibilidades que ofrece.

Una Blockchain es una gran base de datos que, a diferencia del resto, no se encuentra en un sitio fijo ni controlada por un ente centralizado. Esta está distribuida por todo el mundo en diferentes nodos o servidores que poseen una copia de la base de datos y participan dentro de la red. Como su nombre indica, Blockchain significa "cadena de bloques". Las bases de datos que estamos acostumbrados a ver son lineales, en cambio, esta tecnología se divide en bloques que contiene un determinado número de transacciones. Conforme nuevas transacciones entren a la base de datos, más bloques se crean.

En el sistema bancario tradicional, las personas autorizadas pueden rechazar transacciones e incluso eliminar algunas hechas mucho tiempo atrás, pudiendo ser manipulado. Mientras que la Blockchain, al ser descentralizada, nadie pueda eliminar o modificar ninguna transacción realizada, cada bloque producido tiene información del bloque anterior. Esto consigue que la Blockchain sea inmutable.

Además, debemos añadir que, bajo el sistema tradicional, el banco se lleva una comisión por transacción y manutención de tu cuenta y tienen la capacidad de crear dinero de forma ilimitada, por lo tanto, hay una inflación no controlada. No podemos llegar a saber jamás cuantos euros o dólares habrá en circulación, ya que depende de las políticas monetarias de los gobiernos, la situación económica y muchos otros factores. La tecnología Blockchain soluciona este problema de forma eficiente ya que no hay ninguna empresa, gobierno, banco o entidad detrás, teniendo una inflación fija,

[12] NAKAMOTO, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* BITCOIN.ES [consultado 28/01/2021]. Disponible en: https://bitcoin.org/bitcoin.pdf

controlada y predecible. Nuevos Bitcoins se producen cada vez que se genera un bloque, pudiendo saber cuántos habrá en un futuro.

Como se ha indicado anteriormente, los datos no están centralizados, sino compartidos con todos los usuarios de la red, pero entonces ¿quién verifica que las transacciones sean legítimas y que no hay fallos dentro de la red? ¿quién decide el desarrollo de esa criptomoneda? Para entender el funcionamiento, debemos hablar de la tecnología de intercambio de datos **peer-to-peer**. Esta conecta distintos usuarios que comparten información, por tanto, en el momento en que se realiza una transacción, se transmite un bloque de datos a toda la red con el objetivo de validarla.

La transacción es el movimiento de un activo y el bloque elige la información que registra (qué, quién, cuándo, cuánto, dónde y cómo). Existe una conexión entre los bloques con sus anteriores y posteriores, formando una cadena. Cada bloque adicional refuerza la verificación del anterior y elimina la posibilidad de ser manipulado, hecho que hace que esta tecnología permita crear una especie de registro imborrable.

La estructura de estos bloques es una estructura de datos en árbol, permitiendo que un elevado número de datos separados se relacionen con un único valor **hash**, proporcionando un método de verificación eficiente de los datos almacenados.

Respecto a la generación de estos bloques se necesita un consenso distribuido en el que los nodos tengan la capacidad de generar datos válidos. Los **nodos** hacen referencia a ordenadores con un software determinado que están conectados entre sí, regidos por las mismas reglas, creando una red que mueve toda la información de lo que ocurre en el sistema, con el objetivo de unir bloques. Todos los nodos operan igual, no hay jerarquía, por lo que repiten el proceso con cada nodo agregado y sus decisiones se determinan democráticamente.

De esta forma, se distribuye el poder de decisión y validez de las transacciones agrupándolas en bloques. Sus propios participantes son los que toman las decisiones y nadie puede hackearla. La seguridad aumenta cuantas más personas se unen a la red, dado que más usuarios se convierten en nodos y más justa será la decisión de crear un bloque o no. Estos usuarios competirán entre sí en el momento en que deseen convertirse en “mineros” para crear bloques, ya que son recompensados por la creación de nuevas monedas durante el proceso de “minado”.

El proceso de validación del que se habla está basado en criptografía asimétrica, explicada anteriormente, que cuenta con una clave pública y otra privada. Todas las transacciones emitidas se validan por los nodos en el nuevo bloque minado, así como su correcta vinculación con el bloque anterior. Para que los nodos tengan capacidad de generar datos válidos es necesario un consenso distribuido. De esta forma si alguien intenta vulnerar la seguridad de esta tecnología, deberá poseer al menos la mitad de los nodos o en su defecto sobornarlos.

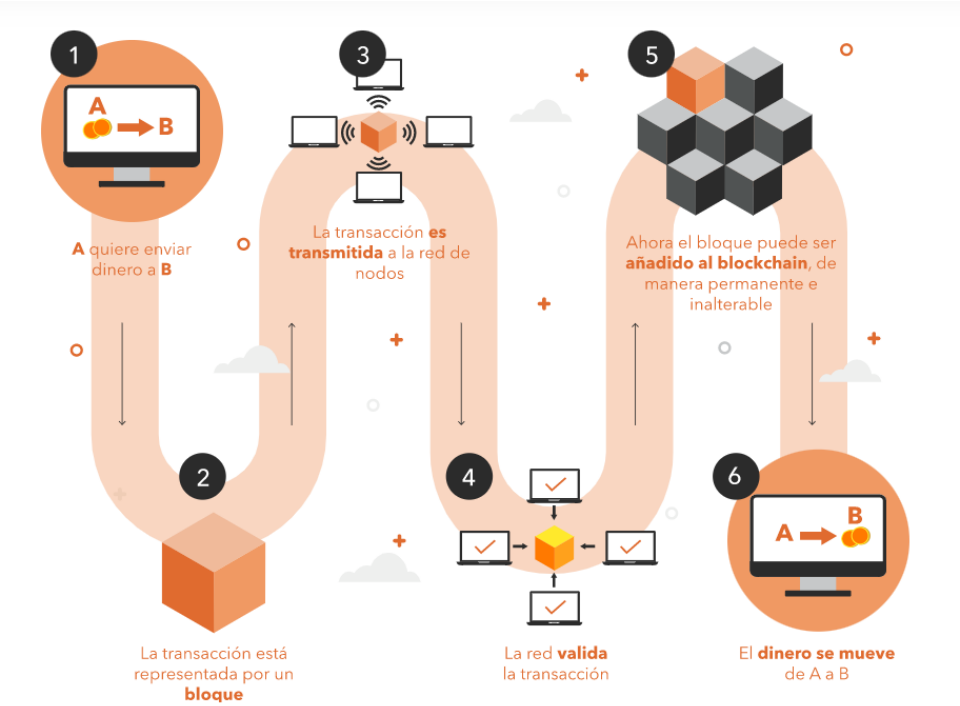

Ilustración 4- Funcionamiento de la tecnología Blockchain
Fuente: Occam

Pero, todo ello no sería posible sin la aplicación de un sistema de consenso. El consenso es parte fundamental del funcionamiento de la tecnología Blockchain, ya que garantiza la seguridad de la cadena de bloques, controlando el hecho de que todos los que participen en la red acepten de forma unánime la información que contiene la cadena. Podría hacerse un símil con una auditoría, impidiendo así que alguien mande información manipulada a la Blockchain.

De no alcanzar un consenso según las normas establecidas en el protocolo para incluir y validar la información dentro de la cadena, se dan situaciones que llevan a realizar bifurcaciones en la cadena: hard fork, duras o soft fork, suaves. Una hard fork hace referencia a una actualización importante del protocolo que obliga a los usuarios a pasar al nuevo software si quieren seguir usando la misma cadena de bloques, es decir, se

produce un cambio en el código que hace que se produzca una "bifurcación de la red", debiendo los usuarios elegir entre usar la versión anterior o la nueva.

Mientras que un soft fork, son pequeñas actualizaciones del software o código del programa que permiten seguir operando, aunque estos no lo actualicen, no alterando las reglas que pudieran romper el funcionamiento de la anterior versión.

Los nodos son los que trabajan en la validación de la información incluida en dicho bloque, creado por los mineros. Se dice que estos son verificadores que hacen Pow (Proof of work), un mecanismo de consenso descentralizado que requiere que los miembros de una red se esfuercen en resolver un rompecabezas matemático arbitrario para evitar que alguien juegue con el sistema.

Esto se consigue a través de lo que se conoce como nonce "number that can be only used once" (número que sólo puede usarse una vez) que funciona en combinación con el hash. El nonce es un número aleatorio que sólo puede usarse una vez con el objetivo de autentificar una transferencia de información entre dos o más usuarios. Además, incluye una variante de tiempo que impide su repetición, generando aleatoriamente un número suficiente de bits que reduzcan la probabilidad de predecirlo. Para calcular el nonce se requieren de grandes cantidades de recursos de cómputo y de tiempo, necesitando por tanto realizar PoW, que confirmen que una determinada combinación de bits da como resultado un hash correcto. El nonce es el número que los mineros tratan de resolver y cuando lo encuentran, estos reciben una contraprestación a cambio.

Si bien es cierto, las funciones hash van de la mano con el nonce, ya que ambos trabajan con el mismo objetivo que es codificar datos como parte de la cadena para agregar seguridad en esta tecnología. El hash responde a una función criptográfica que genera un identificador único e irrepetible a partir de una información dada. Es de especial interés para explicar esta tecnología el hash SHA-256[13] (ver imagen).

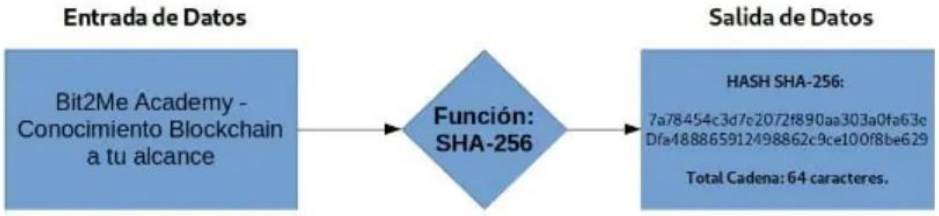

Ilustración 5- Función hash: SHA-256
Fuente: Academy.bit2me

[13] Academy, B. (2021). *¿Qué es un hash?*. BIT2ME ACADEMY. [consultado 17/12/2021]. Disponible en: https://academy.bit2me.com/que-es-hash/

V. CARACTERÍSTICAS DEL BLOCKCHAIN[14]

Entendiendo Blockchain de forma independiente, debemos tener en cuenta ciertas características que deben darse para poder hablar de esta tecnología:

- **Distribuida:** más allá de ser una red descentralizada, es una red distribuida y por tanto, todos los nodos de la red son iguales y cada uno de ellos tiene una copia de la información de la Blockchain.
- **Trazabilidad:** en un principio se puede conocer el origen de la primera transacción, hacer un seguimiento del dinero, es decir, si recibo un Bitcoin puedo ir a la cuenta que me lo ha enviado y puedo seguir ese Bitcoin hasta el minero que recibió la recompensa.
- **Pública:** cualquiera puede ver las transacciones que se realizan
- **Segura:** la información de las transacciones realizadas se almacena en bloques impidiendo la manipulación de información y doble gasto.
- **Inmutable**: esta tecnología está basada en la criptografía, por lo que no se puede alterar la información de un bloque. Si se intentará manipular, se detectaría de forma rápida por el resto de los nodos.
- **Privada/anónima**: Para participar en ella únicamente necesitas acceso a internet y no requiere de identificación alguna. Si bien es cierto, no es del todo correcto indicar que es anónima como tal, ya que actualmente hay gobiernos que están intentando regular plataformas para que los usuarios se deban identificar y así poder hacer un seguimiento de las transacciones para su posterior tributación.
- **Incensurable**: nadie puede impedir que accedas a ella, ya que es una tecnología de código abierto, a disposición de todos (open source).
- **Acuerdos rápidos:** permite a los usuarios efectuar transacciones más rápido a lo que estamos acostumbrados con los sistemas bancarios tradicionales, ahorrando así tiempo en el largo plazo.
- **Consenso:** cada bloque prospera gracias al consenso entre la red y así es como se toman decisiones.

[14] Rodriguez, N. (2019, 14 enero). *6 Características clave de la tecnología Blockchain que debes conocer!*. 101 BLOCKCHAINS. [consultado 12/12/2021]. Disponible en: https://101Blockchains.com/es/caracteristicas-tecnologia-Blockchain/

VI. USOS DE BLOCKCHAIN

En este apartado se explican con diferentes ejemplos los distintos usos que puede tener esta tecnología. Existen miles de criptomonedas y sería prácticamente imposible explicar las diferencias entre cada una de ellas, pero se pueden establecer 3 categorías de criptoactivos: aquellos que basan su proyecto en mantener un valor, los que brindan una utilidad garantizando diferentes usos y tokens respaldados por bienes físicos.

Teniendo en cuenta esta clasificación, en el momento en que existe una moneda que me permite representar valor, titularidad y, además, una infraestructura que me permite moverlas de una forma algorítmica o programable, tengo un sistema financiero completo. Blockchain por esto es disruptivo, no necesito un estado ni gobiernos, sino que a través de esta tecnología se empodera a la gente para que haga intercambios de valor y de titularidad de forma programable en cadenas sin que intervenga el estado.

1. VALOR:

En primer lugar, se explican aquellas monedas que tienen un valor intrínseco (en inglés, "currency"), lo que indica que al intercambiarlas obtengo un valor[15]. La moneda más famosa con diferencia es Bitcoin que nació como una moneda electrónica, pero hay otras que salieron posteriormente como Litcoin, Zcash, Nano, …

Estas son un tipo de divisa como el euro o el dólar, que tienen un valor de mercado. Todas ellas se escriben en una base de datos que es Blockchain (cadena de bloques). Las principales ventajas que me da usar este tipo de respaldo, en lugar de un banco central, son: **inmutabilidad**, ya que la transacción se escribe en un bloque y una vez escrito podré tenerlo a priori eternamente. Funciona de una forma particular a través de una base de datos escrita millones de veces por miles de mineros por todo el planeta. I**ncesorables**, ya que no se necesita permiso o autorización de ningún tipo para escribir algo en la cadena, es decir nadie me puede requerir nada y además, son **monedas nativamente globales**, por lo que hacer una transacción con China no es problema, no tienen concepto de país, existen en un plano digital donde no hay noción de estado y **públicas**, la propia sociedad puede ver todo lo que se escribe en la cadena, es

[15] FERRUZ AGUDO, L. y RIVAS, J. (2021). *Fraude Codicia Ignorancia: Las burbujas financieras en los mercados*. España: Independently Publisher

opensource, si fuera un desarrollador podría proponer cambios e influir en el desarrollo de la moneda.

i. Políticas monetarias vs criptoactivos

Las criptomonedas son tan sólo uno de los proyectos de Blockchain y Bitcoin no es más que una de las más de 10.000 criptomonedas o monedas virtuales que existen en todo el mundo[16].

Es complicado saber el número concreto de criptomonedas que existen actualmente en el mercado, ya que se generan y se destruyen anualmente muchas de ellas y no existe una única base de información acerca de las mismas debido a que cada una de forma individual negocia su publicación en las diferentes aplicaciones. Es por ello, que podemos utilizar la evolución de la capitalización del mercado de las criptomonedas, que alcanzó los 3 billones de dólares en noviembre de 2021, frente a los 620.000 millones en 2017[17], y partir de la información que nos puede ofrecer algunas aplicaciones.

Ilustración 6- Capitalización total del mercado de criptomonedas

Fuente: Coinmarketcap.com

Ilustración 7- Información global de Coinmarketcap.com

[16] SAEZ HURTADO, J. (2021, 8 agosto). Las 10 criptodivisas (o criptomonedas) con más futuro. IEBSCHOOL [consultado 18/01/2022]. Disponible en: https://www.iebschool.com/blog/criptodivisas-criptomonedas-invertir-finanzas/#:~:text=Hoy%20en%20d%C3%ADa%20existen%20m%C3%A1s,y%20la%20filosof%C3%ADa%20que%20utilizan.

[17] *Cuadros de criptomoneda mundial- Capitalización total del mercado de criptomonedas* [consultado el 13/02/2022] en COINMARKETCAP. Disponible en: https://coinmarketcap.com/es/charts/

El Bitcoin es una criptomoneda que busca crear valor, basándose en al oro, al igual que el oro el número de Bitcoins que van a existir es finito, concretamente 21 millones, y necesitan al igual que este, ser minados. El Oro precisamente mantiene su valor porque es un bien escaso y el Bitcoin en cierta manera imita sus funciones dándole el beneficio de la facilidad para realizar transacciones y un carácter deflacionario, al haber cada vez menos Bitcoins en circulación y al crecer su demanda.

Está previsto que se llegue a 21 millones en 2140[18], pero es difícil de predecir ya que el algoritmo de creación de Bitcoin es completo y el ritmo de generación de criptomonedas en el proceso de minado se ralentiza con el paso del tiempo.

Es interesante plantear esto ya que explica la gran diferencia con las políticas económicas actuales. El minado de criptomonedas por parte de los usuarios es un proceso distribuido y radicalmente distinto a la emisión de divisa por parte de un banco central, debido a que los estados pueden emitir sin límite, mientras que, la masa monetaria de criptomonedas como Bitcoin está predefinida.

Para entenderlo, pongamos un ejemplo comparando el sistema del USD (dólar) con el sistema de Bitcoin. A día de hoy, hay más de 19 millones de Bitcoin minados[19], por lo que si compramos el 25% tenemos casi 5 millones de Bitcoin que seguirán teniendo ese valor en cualquier momento, mientras que si compras el 25% de todos los USD que hay actualmente (imaginemos que hay unos 3 trillones de dólares), dentro de 20 años ya no tendré el 25% porque habrá más en circulación, por lo que igual tendré un 12,5% de USD. En este contexto, el Bitcoin revoluciona el concepto de política monetaria, que si tiene algo malo es que siempre hay alguien que imprime más. Con todo esto se quiere

[18] Nieto, A. (2018). *El número de Bitcoins es finito, no podrá haber más de 21 millones: ¿qué se espera que suceda entonces?*. XATAKA. [consultado 17/12/2021]. Disponible en: https://www.xataka.com/criptomonedas/el-numero-de-Bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces
YOUNG, M. (2021, 13 enero). ¿Cuántos de los 21 millones de Bitcoin quedan?. BEINCRYPTO. [consultado 13/02/2021]. Disponible en: https://es.beincrypto.com/cuantos-21-millones-bitcoin-btc-quedan/
ROSEN, P. (2021, 15 diciembre). *El 90% de los bitcoin ya han sido minados, pero el 10% restante tardará 120 años en llegar al mercado.* BUSINESS INSIDER. [consultado 13/02/2022]. Disponible en: https://www.businessinsider.es/cuantos-bitcoins-han-minado-ya-980561
MUÑOZ CABANES, A. (2021, 4 enero). *¿Qué diferencias hay entre una moneda digital y una criptomoneda?*. BBVA Communications. [consultado 22/12/2021]. Disponible en: https://www.bbva.com/es/que-diferencias-hay-entre-una-moneda-digital-y-una-criptomoneda/
[19] iProUP (2021, 13 diciembre). *Sólo resta el 10% de Bitcoin por minar: ¿cuándo se obtendrá el último BTC?*. ECONOMÍA DIGITAL iProUP [consultado 20/01/2022]. Disponible en: https://www.iproup.com/economia-digital/28169-bitcoin-cuantas-unidades-quedan-aun-por-minar

hacer hincapié en que esto no sólo es algo en lo que poder invertir, sino que puede modificar el sistema financiero tal y como lo conocemos.

Si es cierto, a pesar de las ventajas que pueda tener, existen múltiples riesgos, principalmente la volatilidad de este mercado, que tal y como lo conocemos es meramente especulativo. Precisamente la CNMV emitía un comunicado junto con el Banco de España sobre el riesgo de las criptomonedas como inversión[20], indicando su extrema volatilidad, complejidad y falta de transparencia. En este comunicado se indicaba la falta de regulación y por tanto de garantías, así como la propuesta del reglamento a nivel europeo (conocido como Reglamento MiCA[21]) como marco normativo básico. Hace referencia a la falta de consideración como medio de pago al no cumplir adecuadamente las funciones de unidad de cuenta y depósito de valor, y la inexistencia respaldo de un banco central u otra autoridad pública, así como de un mecanismo de protección. Además, pequeños ahorradores que se pueden ver atraídos deben ser conscientes del componente especulativo que los puede llevar a la pérdida total de la inversión e incluso de la carencia de liquidez que existe detrás de ella. Esto sin todavía indicar los problemas derivados del carácter transfronterizo que impiden localizar ciertos criptoactivos en caso de necesitar resolver un posible conflicto, así como los riesgos específicos que puede suponer la custodia de criptomonedas en monederos o wallets en caso de robo, estafa o pérdida.

Es por ello, que frente a este sistema se debe analizar la reacción de los bancos centrales que proponen en un futuro cercano la creación de monedas digitales públicas, lo que supondría un punto de inflexión con sistema actual y un cambio que afecta directamente a las monedas digitales privadas. En la siguiente ilustración se observa geográficamente los bancos centrales que han tomado cartas en el asunto emitiendo su propia moneda.

[20] CNMV (2021, 9 febrero). Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión. CNMV y BANCO DE ESPAÑA. [consultado 13/01/2022]. Disponible en: https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D

[21] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. Comisión Europea. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593&from=NL

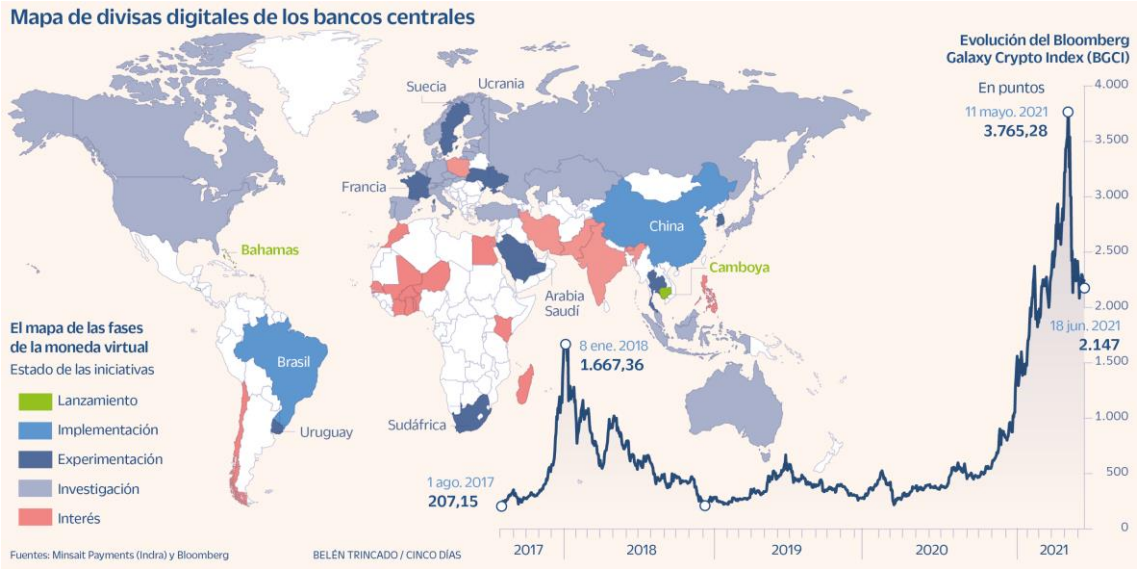

Ilustración 8- Mapa de divisas digitales de los bancos centrales (actualizado 18/06/2021)

Fuente: Cinco Días, El País

Desde julio de 2021 se puso en marcha el proyecto de emisión de monedas digitales por los bancos centrales (CBDC) con el objetivo de combinar la eficiencia de un instrumento de pago digital con la seguridad del dinero de banco central[22]. No viene a sustituir al efectivo, sino a complementarlo, ya que su papel se ve desafiado por la digitalización. Por ello, este proyecto consiste en dar la posibilidad de que se comience a utilizar el dinero del banco central para los pagos digitales al por menor, manteniendo un buen funcionamiento de los pagos, aportando estabilidad monetaria y financiera[23].

En conclusión, las divisas tradicionales están controladas por estados, el ritmo de impresión de dinero lo decide el banco central. Por tanto, si tengo dólares estoy dispuesto a lo que decida la Reserva Federal respecto al tipo de interés o al ritmo de impresión del dinero. Bitcoin, como muchas otras monedas, lo que ofrece es una moneda no sujeta a las decisiones de un estado.

Si bien es cierto, no podemos olvidar que en momentos de crisis este tipo de políticas permiten tener cierta seguridad ya que existe detrás un respaldo. Precisamente el hecho de no estar respaldadas por una entidad legal hace que su volatilidad sea elevada, ya que

[22] La presidenta del BCE, Christine Lagarde decía: «Nuestro trabajo trata de garantizar que, en la era digital, los ciudadanos y las empresas sigan teniendo acceso a la forma de dinero más segura, el dinero de banco central». ECB. (2021, 14 julio). *El Eurosistema pone en marcha el proyecto de un euro digital*. ECB.EUROPA Nota de Prensa. [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.es.html

[23] PANETTA, F. (2021). *Un euro digital*. EBC. EUROPA [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/paym/digital_euro/html/index.es.html

mientras los bancos centrales velan por la estabilidad financiera a través de políticas monetarias con relación a otras divisas, el Bitcoin es una moneda poco predecible al actuar en un mercado inmaduro, no respaldado y lleno de expectativas.

En este sentido, Natalia Español, economistas del BBVA, indicaba[24]: "desde un punto de vista económico, las criptomonedas nativas de redes descentralizadas, como Bitcoin o Ethereum, no están ancladas al valor de una moneda de curso legal, sino que están sujetas al precio que marquen la oferta y la demanda. Además, hay que tener en cuenta que no están respaldadas por una entidad legal que responda en caso de darse problemas técnicos".

Frente a esto, aparecen las CBDC con la idea de seguir manteniendo la confianza en el euro con el sentido de unicidad que nos aporta, ya que al fin y al cabo en muchas ocasiones la confianza en el dinero privado se basa en la capacidad de convertirlo a dinero del banco central, al ser la forma más segura de dinero disponible por el momento[25]. El dinero del banco central nos proporciona un ancla monetaria indiscutible, mientras que habría que vigilar la solidez de los emisores privados para evaluar el valor de cada forma de dinero privado, socavando ese sentimiento de unicidad sobre cualquier moneda.

Incluso el Fondo Monetario Internacional (FMI) indicaba hace unas semanas el riesgo de la creciente desestabilización del sistema financiero internacional con criptomonedas como Bitcoin, Ethereum o Cardano, entre otras, dada la popularidad y el elevado valor de mercado que han alcanzado. Además, el FMI destaca que la correlación de las criptomonedas con inversiones tradicionales como la renta variable ha aumentado significativamente, lo que limita los beneficios percibidos de la diversificación del riesgo y aumenta el riesgo de contagio en los mercados financieros. Se considera esencial adoptar un marco regulatorio global para guiar la normativa y mitigar los riesgos que estos activos puedan suponer[26].

---

[24] E. (2021, 4 enero). ¿Qué diferencias hay entre una moneda digital y una criptomoneda? BBVA RESEARCH. [consultado 16/11/2021]. Disponible en: https://www.bbva.com/es/que-diferencias-hay-entre-una-moneda-digital-y-una-criptomoneda/

[25] PANETTA, F. (2021, 19 noviembre). *The ECB's case for central bank digital currencies*. ECB.EUROPA [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog211119~fda94a3f84.es.html

[26] EUROPAPRESS (2022, 11 de enero). *El FMI alerta de la capacidad de los criptoactivos para desestabilizar los mercados e insta a regularlos.* Economía - EUROPAPRESS [consultado 13/02/2022]. Disponible en: https://www.europapress.es/economia/finanzas-00340/noticia-fmi-alerta-capacidad-criptoactivos-desestabilizar-mercados-insta-regularlos-20220111174039.html

ii. Ejemplo Bitcoin

En la actualidad continuamente se habla de criptomonedas, pero es cierto que la más escuchada es el Bitcoin. Se define "Bitcoin" como un medio de intercambio electrónico o moneda virtual que sirve para adquirir productos y servicios como con cualquier otra moneda. Previamente habían existido otros proyectos de criptomonedas, pero con esta se consigue corregir el problema del doble gasto, es decir, la posibilidad de usar dos veces la misma cantidad de monedas sin que quede registro de un primer uso, a través de la prueba de trabajo (PoW).

Esta es una moneda descentralizada, sin ente de control responsable de su emisión y registro de sus movimientos. Consiste en una clave criptográfica que se asocia a un monedero virtual que descuenta y recibe pagos.

Para poder hacer un intercambio, cada usuario debe tener una clave criptográfica y el sistema permite que en el monedero de cada usuario aumente la cantidad de Bitcoin conforme se realizan compras y disminuya conforme se realiza una venta. Es importante indicar que en estas transacciones no existen intermediarios y tienen un funcionamiento ininterrumpido 24 horas.

Además, tener en cuenta que la moneda y la clave asociada al código criptográfico deben ser verificados para ejecutar las transacciones en base a un sistema de consenso descentralizado. Detrás de este proyecto está la tecnología Blockchain, explicada con anterioridad, que permite empaquetar la información de la red en bloques que se emiten casa cierto tiempo y se les aplica una prueba de trabajo que crea un hash único para cada bloque. Cabe mencionar que este hash es un eslabón que relaciona el bloque anterior con el siguiente dentro de la red. El proceso de minería en Bitcoin busca realizar una serie de complejos cálculos matemáticos que son usados para la validación de las transacciones. Estos cálculos exigen un enorme poder de cómputo que ha evolucionado con el tiempo, llegando a necesitar un equipo especializado para ello. Dado el completo trabajo que esto supone a los miremos se les recompensa con la entrega de Bitcoins según la cantidad de trabajo aportado.

Una de las principales características de esta moneda digita es su emisión. Como se ha comentado anteriormente, la emisión máxima de Bitcoin no superará los 21 millones de BTC. El Bitcoin tiene capacidad de subdividirse hasta los 8 decimales, por lo que 1 unidad de Bitcoin puede fraccionarse hasta en 100.000.000 de unidades pequeñas.

La emisión se realiza a través de un algoritmo. Cada bloque se genera cada 10 minutos, es decir, en ese tiempo los mineros incluyen una serie de transacciones, resuelven el acertijo criptográfico del bloque y lo trasmiten a la red. El que logre resolver el "acertijo" recibe una recompensa que es la que permite introducir nuevas monedas en el mercado. Esta recompensa disminuye cada 210.000 bloques que se crean, lo que se debe a un proceso conocido como holding donde el objetivo es controlar la inflación del Bitcoin y convertirla en una emisión deflacionaria. En la actualidad cada bloque validado tiene una recompensa de aproximadamente 12, 5 BTC[27].

En la actualidad llama la atención el elevado consumo de energía que supone la emisión de esta criptomoneda, hecho que se debe a la prueba de trabajo (PoW) y que supone un grave problema ambiental con la mayoría de las monedas digitales privadas. Este sistema consume grandes cantidades de energía, pero ciertamente logra un nivel de seguridad tal que es prácticamente imposible hackearlo. Precisamente por esta razón se eligió este sistema como protocolo de consenso de Bitcoin.

2. UTILITY

El segundo grupo son las monedas de utilidad, en inglés "utility token". Ethereum es el claro ejemplo para entender esto. Esta criptomoneda también opera sobre una cadena de bloques, pero tiene una particular diferencia, y es que además de permitir transacciones entre usuarios (ETH), le puedo mandar estos ETH a algoritmos o bots. Estos algoritmos se escriben en bloques y todas las características que me da Blockchain las tengo no sólo en la trasferencia entre usuarios, sino también en el proceso a algoritmos. Cuando escribo un algoritmo, sigue funcionando de la misma forma idéntica eternamente.

Por ejemplo, si dos personas establecen un acuerdo para crear una web que da servicios de asesoramiento donde uno es el programador y otro hace los contenidos. En dicho acuerdo se establece que todo el dinero que genere esa web se reparte de forma que el programador se lleva el 60% y el creador de contenidos el 40% de los beneficios. Se crea un "smart contract" muy sencillo y se dice a la gente que visite la web que mande dinero a una dirección, donde no habría una persona sino el algoritmo. El algoritmo tiene una rutina sencilla y cuando recibe el dinero lo parte en dos, 60% lo manda al

[27] Academy, B. (2021, 13 julio). *¿Qué es Bitcoin (BTC)?*. BIT2ME ACADEMY. [consultado 18/11/2021]. Disponible en: https://academy.bit2me.com/que-es-Bitcoin-btc-criptomoneda/

programador y el 40% al del contenido. Como esa dirección está vinculada a un bloque específico, tengo la garantía de que ese algoritmo se va a ejecutar.

Pero ¿dónde se ejecuta ese algoritmo? El que hace la división se le tendrá que compensar de alguna forma, y en el caso de Ethereum se le compensa con "gas" (término en inglés que se utiliza para referirse a gasolina). Este ordenador que ejecuta los algoritmos necesita algo para que funcione, este gas son ETH.

Cuando compro Bitcoin compro la habilidad de crear un valor, mientras que cuando compro Ethereum compro el gas que hace que la máquina funcione.

Otro ejemplo mucho más sencillo incluso podría ser el de los autos de choque en las ferias. Debías comprar unas monedas/fichas en una caseta y sólo con ellas funcionaba el coche durante unos minutos por una pista cerrada. Estas monedas de utilidad se pueden entender así, teniendo en cuenta que lo que se hace es comprar ejecución en una cadena de bloques.

i. Ejemplo Ethereum como plataforma y concepto de "Gas"

Ethereum es uno de los proyectos de criptomoneda más grande de la industria. Es una plataforma digital que se basa en la tecnología Blockchain o cadena de bloques, capaz de ejecutar numerosas aplicaciones descentralizadas, contratos inteligentes y soportar miles de tokens. Para lograr esto, este proyecto cuenta con una red y una criptomoneda con características únicas.

La moneda de esta red se denomina Ether (ETH) y de forma similar a Bitcoin (BTC), no está controlada por ningún organismo ni gobierno regulador. Su desarrollo es descentralizado y está marcado por la Fundación Ethereum y la comunidad que lo apoya. A pesar de utilizar actualmente el protocolo de consenso de PoW, está dando un salto a través de un protocolo Proof of Stake (PoS), hacia el sistema de Prueba de Participación con su actualización Ethereum 2.0.

A continuación, se citan alguna de las principales características técnicas de esta criptomoneda. La minería, es decir, el uso del protocolo de PoW y el uso del algoritmo Ethash, lo que aporta seguridad a la red. Sin embargo, cambiará el protocolo eliminando la minería por el staking y los validadores en la red. La emisión es clave, ya que actualmente cuenta con una emisión anual limitada a 18 millones de ETH, sin embargo,

la emisión total de la moneda es infinita. Además, a diferencia de Bitcoin, si un minero recibe la solución de un bloque recibe una recompensa de 2 ETH, pero si a su vez otro encuentra una solución posible, recibirá también una recompensa.

El gas, es la base de esta criptomoneda y se utiliza para medir el trabajo realizado dentro de la Blockchain. Cada acción en Ethereum, como una operación o un conjunto de ellas, tiene un coste especifico en unidades de gas, por eso se le conoce como su combustible. Las funciones del gas son asignar un coste a la ejecución de tareas, el precio que hay que pagar por realizar acciones dentro de la plataforma; ayudar a mejorar la seguridad del sistema, cada acción tiene un precio lo que permite proteger la red frente ataques de spam ya que sería muy costoso; y finalmente, recompensar a los mineros, que cobran tarifas de gas por la ejecución de transacciones de la red.

Actualmente el límite de tamaño de cada bloque en esta plataforma es de 12,5 millones de gas, por lo que cada bloque puede contener un total de operaciones siempre y cuando no sobrepase el límite de gas especificado. Además, en cuanto al tiempo de generación de bloques es mucho más rápida que Bitcoin, generando un bloque cada 14 segundos.

Alguno de los usos más relevantes de esta criptomoneda son la aceptación y recepción de pagos de forma rápida y segura, gracias a la producción de bloques en segundos, la realización de ICO´s, ya que ofrece herramientas para facilitar la creación de tokens ERC20[28] y por tanto permite crear ofertas iniciales de monedas. En la actualidad existen al menos 191 mil tokens de este tipo, cada uno con características únicas que se ejecutan sobre esta Blockchain.

Otro de los principales usos de Ethereum son los Smart contract y DApps, ambas herramientas con capacidades prácticamente infinitas. Las DApps son aplicaciones informáticas que funcionan en un sistema de computación distribuido, por tanto, completamente descentralizadas, no censurables, seguras y económicamente autosustentables ya que están controladas lo indicado al ordenador en un contrato inteligente. Este contrato del que hablamos o también conocido como Smart contracts

[28] El concepto ERC-20, por sus siglas en inglés Ethereum Request for Comments, responde a un protocolo que consiste en un conjunto de directrices individuales, permitiendo la autorización para ejecutar transacciones de tokens. Es decir, es un protocolo estándar de implementación uniforme de funcionalidad, ofreciendo ventajas como la sencillez para los desarrolladores o la posibilidad de utilizar tokens con softwares de terceros. Los ERC-20 son tokens que se han construido sobre la red Ethereum y la utilizan. Cualquiera puede crear un token y este no siempre se corresponde a una criptomoneda, sólo necesitamos un contrato inteligente para poder crearlo de forma que alguien recibe los tokens si previamente se ha enviado una cantidad determinada de ETH a un Smart Contract que a cambio te envía esos tokens.

son un tipo de cuenta dentro de Etherum que permiten tener un saldo y enviar transacciones por la red. Pueden usarse para crear contratos de compraventa o negociación de bienes o servicios que se ejecutan automáticamente al cumplirse unas condiciones preestablecidas.

3. Security TOKENs

En último lugar, se analizan las llamadas monedas de titularidad, más conocidas por su término en inglés "security token". Tienen un sentido de propiedad, lo que hay detrás de estas monedas es la compra de un activo. Estos criptoactivos están respaldados por activos reales.

Podemos tener "security tokens" que estén respaldados por acciones. Por ejemplo, si tengo una Sociedad Limitada en España con 3 socios donde cada uno tiene el 33% de la compañía, esa información está escrita en el Registro Mercantil, pero este no es ágil. El tiempo y costes relacionados con realizar modificaciones son elevados.

En el mundo de las criptomonedas yo puedo tokenizar y genera unas fichas y escribirlas en un registro público que no depende de un estado, sino de personas (desarrolladores del servicio). Genero estos tokens y los escribo en una cadena de bloques y se da a los propietarios la libertad de que hagan lo que quieran con esos tokens.

Además, las ventajas de los Smart contracts ayudan a agilizar procesos, siendo muy sencillo escribir, por ejemplo, las condiciones bajo las que se aprueba repartir un dividendo y su ejecución inmediata en caso de cumplirse.

Los "Security token" no son más que activos reales cuya titulase reside en el poseedor de la clave privada que les da acceso a los tokens, se puede tokenizar prácticamente todo, siendo posible: deuda, participaciones en fondos de inversión, en empresas, acciones, activos reales (inmuebles), entre otros.

Si bien las criptomonedas Value ponían en jaque al sistema monetario actual, los Security tokens tienen la capacidad de revolucionar el sistema financiero tal y como lo conocemos, puesto que ya no se necesitan bancos como intermediarios para pedir un préstamo o comprar y vender activos financieros. A pesar de ello, bancos centrales y Supervisores están ya en guardia y reaccionando ante estos cambios. De hecho, una de

las opciones para la emisión de CBDC era en la modalidad de token[29], ofreciendo una alternativa eficiente al efectivo para facilitar los pagos, pero esta opción cuenta con el principal inconveniente del anonimato que, si bien es intrínseco al dinero en efectivo, en este caso sería una decisión deliberada que van en contraposición con los mecanismos estipulados para evitar el blanqueo de capitales y la financiación del terrorismo.

i. NFTs

Dentro de este tipo de criptomonedas se deba hacer mención a los NFTs o Non Fungible Tokens (término en inglés, tokens no fungibles). Si bien cualquier cosa se puede tokenizar, es decir, se le puede dar un valor asignado a un modelo de negocio como el de las criptomonedas, no cualquier cosa se puede dividir, es por eso que existe la posibilidad de tokenizar un activo en un único token. Sin embargo, este activo único no se puede modificar ni intercambiar por otro que tenga el mismo valor, por lo que estos NFT´s generalmente se usan para obras de arte digitales considerando también que pueden incluir Smart contracts para generar dinero los creadores a base de Royalties cada vez que haya cambio de titular. Igual que no hay dos cuadros iguales, no hay dos NFT´s, de forma digital se tiene una obra de arte única y por tanto si se quiere comprar sólo puedes adquirir el original. Se les asigna un certificado de autenticidad digital mediante unos metadatos que van recogiendo información sobre el autor, el valor origen y todas las adquisiciones o transacciones que se hayan hecho.

Conviene tener en cuenta por tanto alguna de las características principales de estos tokens como la indivisibilidad, imposibilidad de fraccionamiento que hace que se deban adquirir completamente, aunque su propiedad sí que puede dividirse, la unicidad, activos únicos con rasgos propios y la autenticidad, derivada de la existencia de la red Blockchain en la que se emite donde este es verificado. Además, es relevante tener en cuenta que el concepto de propiedad sobre el token no conlleva necesariamente un derecho de propiedad sobre el activo que el NFT representa, sino que habrá que atenerse a lo establecido en la relación configurada. También, relevante destacar que frente a los activos fungibles donde los estándares Etherum utilizadoses el ERC-20, los NTF

[29] FERNANDEZ DE LIS, S. y GOUVEIA, O. «Monedas digitales emitidas por bancos centrales: características, opciones, ventajas y desventajas». BBVA RESEARCH [revista electrónica], 2019, nº19/03 [consultada 10/01/2022]. Disponible en: https://www.bbvaresearch.com/wp-content/uploads/2019/03/WP_Monedas-digitales-emitidas-por-bancos-centrales-ICO.pdf

utilizan el estándar ERC-721, que incluye unas funciones del propietario otorgando permiso para su transmisión y ciertas propiedades del token que lo distinguen del resto.

El actual crecimiento de los NFT, como se aprecia en la siguiente ilustración, surge de la creencia en un aumento del valor de esos activos con el tiempo y su posterior venta por más dinero. Esto está en auge sobre todo por el tan escuchado metaverso, ya que están estrechamente interconectados. El metaverso es un universo digital que permite a particulares y empresas trasladas activos y servicios del mundo real. Implica una transición hacia vivir cada vez más en la pantalla y no tanto en la realidad, apostando por realizar las cosas del día a día en esta plataforma, ofreciendo una economía abierta, respaldada por la Blockchain.

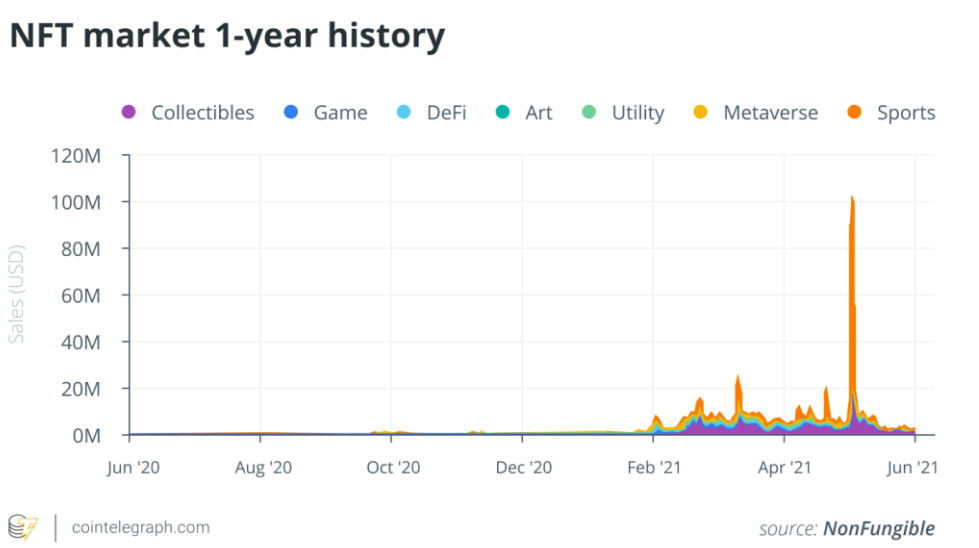

Gráfico 1- Evolución en 1 año del mercado de los NFT

Fuente: Cointelegrah

Por ejemplo, en el metaverso a través de la realidad virtual podrás comprar, interactuar, formarte, etc. Se podrán realizar transacciones a través del metaverso y que se ejecuten en ese mundo virtual o en el real. Imaginemos ahora que queremos operar en el metaverso y queremos montar nuestro negocio. Hay diseñadores de interiores que han creado NFT de espacios como una obra de arte digital y reciben una comisión por cada vez que se utiliza ese diseño. Dentro del NFT este diseñador deja programado un royalty de forma que el cada vez que alguien lo utiliza recibe un 10% de esas transacciones. Y sin irnos más lejos, nuestro jugador o usuario en el metaverso, es decir

nuestra identidad real también estará representada por un avatar de NFT como token de acceso a las diferentes ubicaciones de este mundo paralelo.

Otro ejemplo, aún más ilustrativo si cabe fue la tokenización por primea vez de una portada de un periódico, concretamente la del suplemento del fin de semana en el "XL semanal", de ABC. El artista Javier Arrés diseño la portada exclusivamente para el ABC, logrando un trabajo entre lo artesanal y lo digital y publicándolo mediante un NFT, recogido en Ethereum, saliendo al mercado en las plataformas de la red. La obra se vendió alcanzando un precio de 26.000 dólares[30] en la subasta del 21 de octubre en la plataforma Marketplace con un precio mínimo de venta de 5.000 dólares. Consiguiendo así causar sensación y cierto interés por este mundo como indicaba el criptoautor que decía «espero que la venta de la portada de XLSemanal acerque un poco más el mundo del criptoarte a nivel nacional y se refuerce el mercado del arte NFT español»[31].

Ilustración 9 - La primera publicación NFT de España: historia de la portada

Fuente: XL Semanal

ii. Tokens respaldados por activos físicos

El presidente de la CNMV[32] en uno de sus últimos discursos decía que "las finanzas descentralizadas (…) son en sí mismas positivas (…), en un periodo corto de tiempo, veremos (…) incluso activos reales (inmuebles) tokenizados, formando parte del conjunto de activos en las carteras de los inversores junto con activos tradicionales". Se está produciendo una revolución en el sector inmobiliario con la tokenización de estos activos, facilitando la inversión inmobiliaria al ser esta más sencilla, barata y rápida. Si bien es cierto, el principal problema para que este tipo de inversiones se generalice es la

[30] FERNANDEZ-NESPRAL, Mª., (2021, 24 octubre). *La primera publicación NFT de España: historia de la portada*. XLSEMANAL [consultado 25/01/2022]. Disponible en: https://www.xlsemanal.com/conocer/arte/20211022/portada-xlsemanal-criptoarte-artista-digital-javier-arres-nft.html

[31] ESPÍN, I. (2021, 24 octubre). *ASÍ FUE LA SUBASTA DE LA PRIMERA PORTADA ESPAÑOLA NFT: 23.000 EUROS POR ESTA IMAGEN DE XLSEMANAL*. ABC [consultado 25/01/2022]. Disponible en: https://www.abc.es/xlsemanal/a-fondo/nft-javier-arres-primera-portada-espanola-javier-arres-arte-digital-subasta.html?ref=https%3A%2F%2Fwww.google.com%2F

[32] BUENAVENTURA, R., *Jornada "Retos en un periodo de recuperación"*, 2021, Norbolsa Market Forum organizado por CNMV, Bilbao. Disponible en: https://www.cnmv.es/portal/verDoc.axd?t={b4d3c41d-0f95-493b-9047-88edf03ac8d7}

cuestión regulatoria, además de las características propias de los criptoactivos que plantean riesgos elevados.

Tokenizar un activo inmobiliario viene a significar dividirlo en partes representadas por tokens que poseen el derecho de propiedad. Cada token es digitalizado y puede ser almacenarse en una wallet o transmitirse online de forma inmediata.

Además, cabe indicar que nuestro país se considera como escenario ideal para esta tokenización debido al elevado volumen de negocio del mercado inmobiliario, al nivel de regulación y burocracia ante la compraventa, la necesidad de realizar inversiones y la escasez de liquidez en las mismas[33]. De esta forma el derecho económico sobre el inmueble queda representado en el token, por lo que los inversores que aportan cierto capital para comprar el inmueble reciben tokens que representan su participación. En el momento que decidan ponerlos a la venta, podrán hacerlo a través de un contrato inteligente, en el que el comprador envía criptomonedas y el contrato se ejecuta automáticamente recibiendo este los tokens o manualmente, enviando el token cuando se reciba el pago en dinero FIAT.

[33] TOKENIZA (2020, 14 abril). Cómo es el proceso de Tokenización de un activo inmobiliario. TOKENIZA-Activos en Blockchain [consultado 16/01/2022]. Disponible en: https://www.tokeniza.es/como-es-el-proceso-de-tokenizacion-de-un-activo/
SOLERA, S. (2021, 21 septiembre). *¿Cómo tokenizar un inmueble?* OCCAM. [consultado 16/01/2022]. Disponible en: https://www.occamagenciadigital.com/blog/como-tokenizar-un-inmueble

VII. WALLETS y EXCHANGES

Para poder entender estos conceptos es necesario echar la vista atrás en este trabajo, concretamente en el apartado ***CRIPTOGRAFÍA:*** *¿Cómo funciona el proceso de encriptación?*, donde se mencionan dos claves que son esenciales en el proceso de encriptación asimétrica: la clave pública y la clave privada.

Una wallet o monedero se puede definir como el lugar donde almacenar esa clave privada y poder utilizarla[34]. Técnicamente es un software, de ser online, o hardware, de ser físico, diseñado exclusivamente para almacenar y gestionar dichas claves. Esta herramienta es indispensable ya que nos permite enviar o recibir pagos, ya al hablar de monedas digitales que no existen físicamente y basadas a través de criptografía, de alguna forma u otra tenemos que hacernos con la propiedad y derecho sobre las criptomonedas de realizar ciertas transacciones. Más concretamente los monederos guardan esa clave privada que funciona como una llave otorgando el derecho como propietarios de gastar las criptomonedas contenidas en esa dirección. Como aclaración, las wallets no contiene como tal ninguna criptomoneda, sino que estas se almacenan en una red Blockchain.

Utilizan técnicas de cifrado muy avanzadas para garantizar la seguridad de los usuarios, creando dicha clave privada mediante un algoritmo, siendo prácticamente imposible de adivinarlas. A partir de dicha clave privada se crea la clave pública, relacionadas entre sí matemáticamente, pero imposible de realizar el proceso inversamente, ya que se utiliza un algoritmo unidireccional.

Además, se ha de tener en cuenta que el nivel de seguridad de la wallet dependerá del tipo que sea, por lo que existen diferentes formas de administrar dicha clave privada que se mencionan a continuación.

En primer lugar, las cold wallets o llamadas billeteras frías, que son aquellas que utilizan claves generadas por una fuente no está conectada a Blockchain y, por tanto, tampoco a Internet. Esto hace que sean más seguras, pero soportan un menos almacenamiento de criptomonedas, además de ser costosas. Estas billeteras son físicas y pueden materializarse en cualquier dispositivo o incluso en papel. Las más populares

[34] MARTESANZ, V., (2021, 9 diciembre). *Qué es una wallet de criptomonedas, qué tipos hay y cómo elegir una.* FINECT [consultado 7/01/2022]. Disponible en: https://www.finect.com/usuario/vanesamatesanz/articulos/wallet-criptomonedas-que-es-tipos-como-elegir

son aquellas que requieren un dispositivo como un USB (hardware offline) que tiene incorporado un software.

Dentro de este tipo se conocen las paper wallets como una de las formas más sencillas de monedero. Son un tipo de monedero offline que aporta mayor seguridad que las hot wallet al evitar robos cibernéticos o intrusión de virus. Se trata de un monedero impreso en papel que contiene las claves privadas y direcciones para poder operar. Son mayormente utilizadas para almacenar fondos que van a movilizarse en un largo periodo de tiempo.

Su proceso de creación es muy rápido y sencillo. Tan sólo se debe acceder a un generador, crear la clave privada e imprimir tantas copias como se deseen. Es posible cifrar esta wallet antes de imprimirla, proporcionando una mayor protección. Cabe indicar que esta puede extrapolarse a otros materiales, como, por ejemplo, una placa de metal.

Finalmente, las hot wallets, conocidas por ser gratuitas y digitales, lo que implica que permanecen conectadas a internet y a la red Blockchain de la concreta criptodivisa. Estos monederos se utilizan para enviar y recibir criptomonedas, y permiten ver cuántos tokens se tienen disponibles para usar lo que permite a los usuarios realizar transacciones rápidamente. Al ser monederos online, pueden ser aplicaciones o incluso extensiones del navegador.

A diferencia de las wallets que se utilizan para guardar y gestionar las criptomonedas que tenemos, como una billetera, un exchange sirve para realizar las operaciones de compraventa, es decir, realizar intercambios por dinero FIAT o por otras criptomonedas[35].

Por lo general un exchange hace referencia a un espacio virtual en el que se realizan las transacciones permitiendo al usuario o trader participar en un mercado en el que puede obtener ganancias gracias a la variación de los precios. Estas plataformas posibilitan el movimiento económico y financiero de estos activos a cambio de unas comisiones.

Poco a poco los exchanges de criptomonedas han ido creciendo como se puede apreciar en el siguiente gráfico y actualmente existen múltiples opciones por todo el mundo.

[35] RUS ARIAS, E. (2021, 5 octubre). Exchange de criptomonedas. ECONOMIPEDIA.COM. [consultado 17/12/2021]. Disponible en: https://economipedia.com/definiciones/exchange-de-criptomonedas.html#:~:text=Tenemos%20dos%20categor%C3%ADas%20de%20exchange,otras%20las%20descentralizadas%20(DEX).

Pueden clasificarse en varios grupos según las características y objetivos, aunque siempre como plataformas que facilitan la participación de los usuarios en este nuevo mercado.

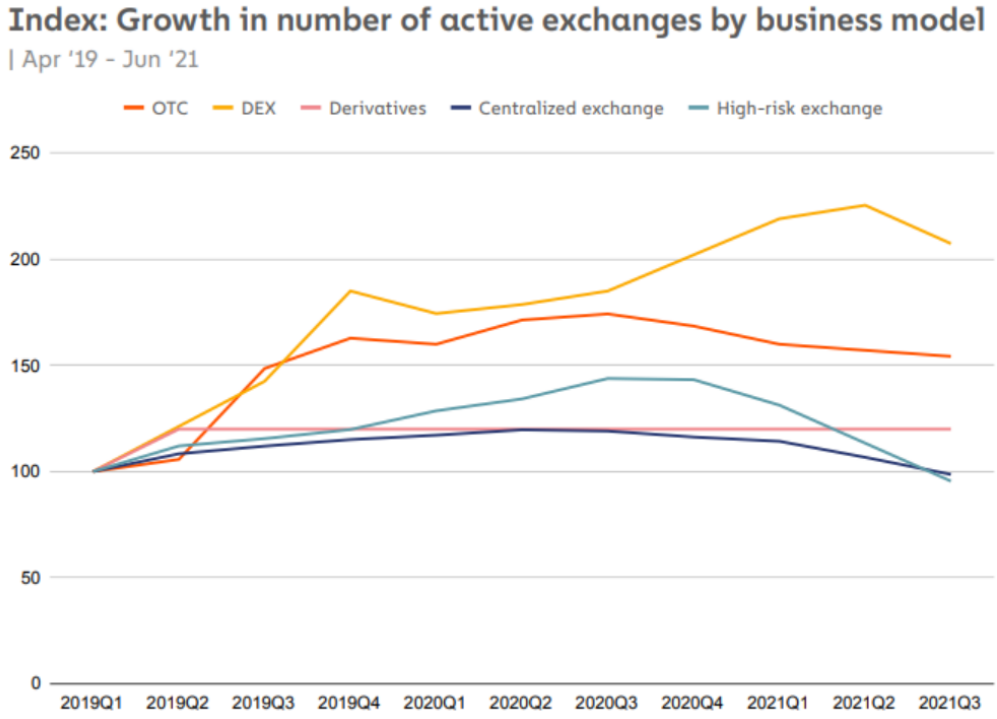

Gráfico 2- Crecimiento del número de exchanges activos según su modelo de negocio

Fuente: Chainalysis

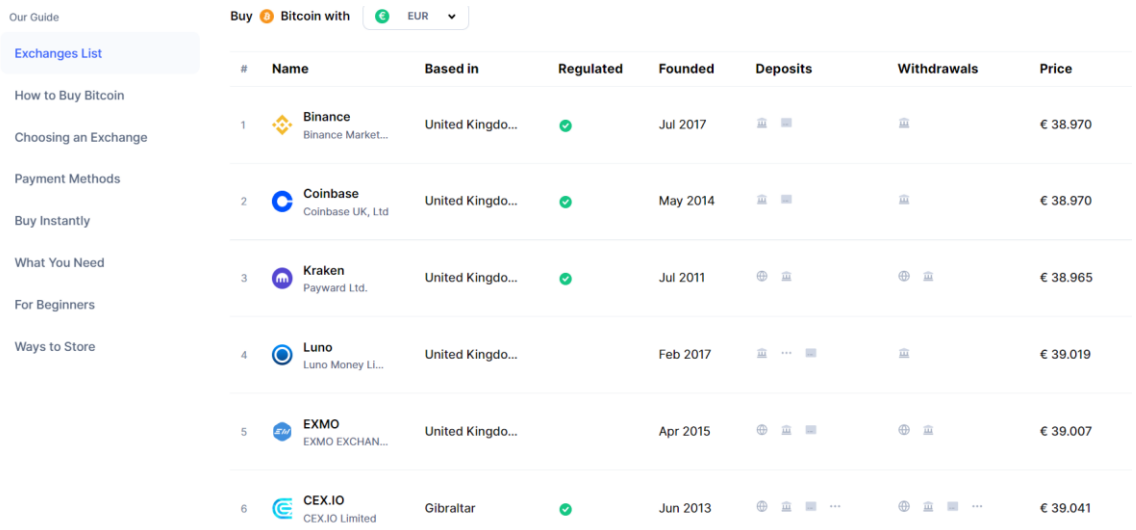

Ilustración 10- Lista de Exchanges para comprar BTC en euros (€)

Fuente: Coinmarketcap.com [actualizado 13/02/2022]

Existen los exchanges tradicionales, como Binance, Coinbase o Kraken, donde los usuarios acceden para la compraventa según la cotización del mercado y suelen ser

plataformas altamente reguladas con un monto mínimo para operar. Generalmente son públicas y el usuario debe dar a conocer su identidad para participar en ellas. Mientras tanto, los exchanges de tipo "bróker" o derivados son plataformas de intercambio entre criptomonedas donde se especula sobre la variación de sus precios como, por ejemplo, Bit2Me o Revolut.

No se puede pasar por alto algunos de los escándalos en los que estas plataformas se han visto inmersos como los robos y hackeos en Binance o las presuntas prácticas de lavado de dinero y delitos fiscales por las que esta misma fue investigada el pasado año[36].

Por otro lado, encontramos las llamadas plataformas OTC (Over The Counter) que ofrecen intercambios punto a punto, garantizando una negociación directa ya que se realizan transacciones que no operan dentro del mercado normal. En este tipo de exchanges son los propios usuarios los que pueden publicar anuncios de compra o venta, fijando ellos mismos las tasas, métodos de pago y condiciones para sus operaciones comerciales[37].

También están los fondos de criptomonedas, iniciativas por profesionales que permiten al usuario comprarlas a través de un este, sin la necesidad de almacenarlas o comprarlas por sí mismo. En ocasiones este tipo de exchange limita la privacidad y puede no ser seguro al no controlar la gestión de los fondos.

Y finalmente, los exchanges descentralizados o comúnmente denominados DEX, entre los que están, por ejemplo, Uniswap o CoinEx. Estos son plataformas similares a los exchanges tradicionales, pero se diferencian en su funcionamiento interno, ya que estos se autogestionan gracias a la programación y en ocasiones permite al usuario tener un elevado nivel de privacidad e incluso anonimato. Estas plataformas se gestionan directamente en la Blockchain mediante Smart Contracts.

---

[36] RAEVENLORD, (2021, 14 mayo). *Binance, World's Largest Crypto Exchange, Reportedly Under Investigation by DoJ, IRS.* TECHPOWERUP. [consultado 13/02/2022]. Disponible en: https://www.techpowerup.com/282228/binance-worlds-largest-crypto-exchange-reportedly-under-investigation-by-doj-irs

[37] WEHOLDERS (2021, 7 junio). COMPARATIVA: Los 3 MEJORES EXCHANGES de CRIPTOMONEDAS [+1 por si eres EMPRESA]. WEHOLDERS- Inversión en bolsa. [consultado 26/01/2022]. Disponible en: https://weholders.com/comparativa-los-3-mejores-exchanges-de-criptomonedas-1-por-si-eres-empresa/#Exchanges_P2P

Dada toda esta información se aconseja valorar el tipo de exchange, así como el wallet elegido, en función del objetivo de la inversión en relación con el proyecto de la criptomoneda para evitar sorpresas.

VIII. OTRAS FORMAS DE MONETIZAR EL BLOCKCHAIN

La tecnología Blockchain ha llegado para transformar nuestras vidas como una tecnología de vanguardia que crece por momentos y así lo ha reflejado en la siguiente gráfica la Organización Mundial del Comercio[38]. Existe un desconocimiento generalizado por gran parte de la población, pero no significa que muchos no se sientan atraídos por las nuevas posibilidades que abarca. A continuación, se analizan diferentes formas de monetizar la tecnología, muchas de ellas ya mencionados a lo largo del trabajo y otras todavía poco conocidas.

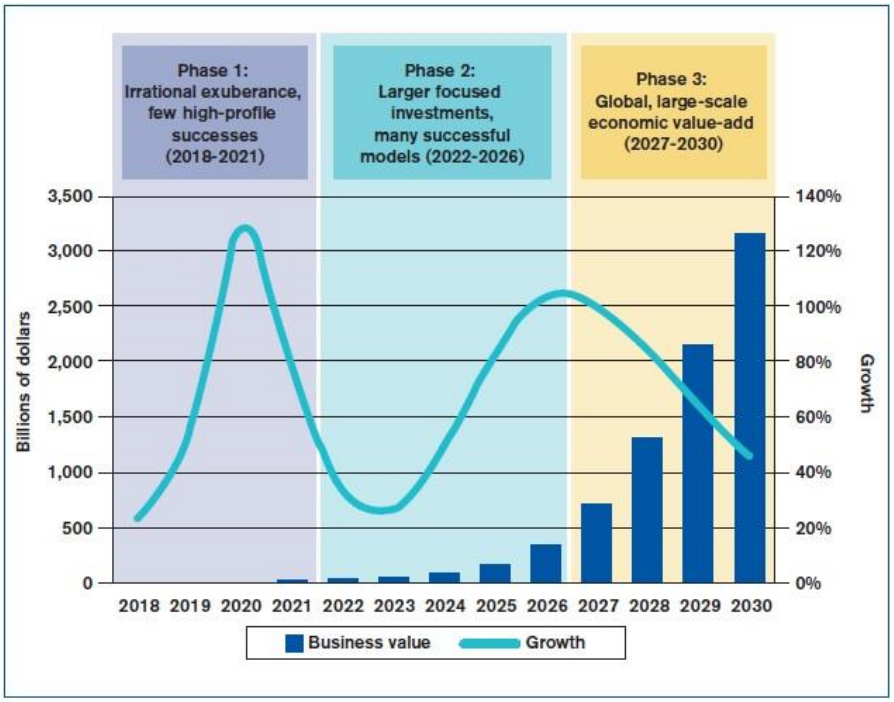

Gráfico 3- Previsión de crecimiento y alcance empresarial de Blockchain analizado en 3 fases en base a la curva de Gartner[39]

Fuente: WTO Publications

Sin lugar a duda, la forma más clara de monetización es a través de la especulación, concretamente con respecto a las criptomonedas, al igual que se especula en bolsa. Todo ello basado en la confianza de un proyecto detrás de una Blockchain, es decir, adquirir una moneda esperando a que se revalorice. Se intenta perseguir lo que de forma coloquial entendemos como "Buy low, sell high" (comprar bajo, vender alto). En este

[38] GANNE, E. «Can Blockchain revolutionize international trade?» WORLD TRADE ORGANIZATION Publications [revista electrónica], 2018 [consultado 28/01/2022]. Disponible en: https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf

[39] Curva de Gartner indica de forma representativa la madurez y adopción de las tecnologías y apps y cómo son potencialmente relevantes para resolver problemas comerciales reales y aprovechar nuevas oportunidades. Disponible en: https://www.gartner.es/es/metodologias/hype-cycle

sentido en ocasiones no sólo se invierte con la idea de comprar para posteriormente al venderlo convertirlo en dinero FIAT y tener una ganancia, sino también con la finalidad de almacenar dinero sin intermediación a través de la compra o intercambio de criptomonedas. Es relevante tener en cuenta la posición legal y tributaria en la declaración del IRPF respecto a las ganancias de la venta de criptoactivos, ya que únicamente se tributa por ellas en el momento en que se conviertan a dinero de curso legal.

Seguidamente uno de los nichos más rentables es la minería. La red está compuesta por nodos u ordenadores que deben verificar las transacciones y participar en la emisión de nuevas criptomonedas, actividad por la que son recompensados. La minería utiliza el mecanismo citado anteriormente de PoW a través de ordenadores con potentes tarjetas gráficas. Se puede distinguir entre el minero que realiza esta actividad individualmente o el conjunto de ellos que trabajan de forma cooperativa para minar bloques de criptomonedas a través de los pools de minería, de forma que la recompensa se divide entre todos los que forman este espacio.

En esta misma línea también es posible participar en los protocolos de consenso y hacer lo que se denomina “Staking” para ganar ciertos ingresos indirectamente. Este proceso consiste en apostar las criptomonedas de las que se es propietario para agregar nuevos bloques a la cadena a cambio de una recompensa que se deposita en su wallet. Es similar a lo que hacen los mineros, pero en vez del mecanismo de Pow, se utiliza el consenso de prueba de participación. De esta forma los usuarios congelan ciertos fondos como garantía y pasan a ser un verificador. Si se identifica como un nodo malicioso, los fondos congelados se le quitan y se reparten entre los nodos buenos, consiguiendo así seguridad en la cadena. Gracias a los efectos de red se consigue un sistema basado en la confianza. La ventaja más significativa frente a la minería es el menor consumo de energía, reduciendo así el impacto ambiental negativo que causan las criptomonedas.

Alternativamente encontramos ciertas ventajas y formas de monetizar esta tecnología a través de las finanzas descentralizadas (DeFi), ofreciendo transacciones financieras entre P2P sin un intermediario. Consisten en una serie de protocolos en la Blockchain que sirven para invertir en criptomonedas mediante depósitos de inversores. Aparece el concepto de liquidity provider o proveedor de liquidez, como un usuario que financia un fondo con criptoactivos de su propiedad para facilitar la negociación en una plataforma

Blockchain y obtener ingresos pasivos por su depósito. Hay mucho riesgo, pero la rentabilidad es muy elevada.

También cabe atender a un concepto que, aunque mencionado anteriormente, se considera relevante tenerlo en cuenta como una nueva forma de monetización de los creadores de contenido, los NFT´s. El crecimiento acelerado de esta tecnología ha hecho que actualmente se realicen copias digitales de una pieza de contenido que puede adquirirse a través de la Blockchain de todo tipo de cosas como patentes, textos, fotos, diseños, ropa, entre otros. Como propietario de un NFT se recibe un certificado de propiedad y cada vez que tu obra se utiliza o lo que es lo mismo alguien la compra, se adquieren unos ingresos. Por ejemplo, 3LAU lanzó el primer álbum musical de la historia vendido como NFT y generó más de 11,6 millones de dólares[40].

Para concluir, suscita cierto interés la posibilidad de beneficiarse de la inversión en empresas que usan estos protocolos. Es decir, a través de estrategias de diferenciación hay muchas empresas que se han introducido en esta tecnología, incorporando Blockchain en fases de la cadena de valor, por lo que, si realizamos una inversión directa en estas empresas y creemos en un futuro próspero respecto a la misma, es posible que acabemos también obteniendo beneficios gracias al crecimiento de estas empresas por sus ventajas competitivas.

Dada la relevancia de esta última visión de la cadena blockchain, aplicada a la economía productiva no especulativa, se indican a continuación alguna de sus posibles aplicaciones y las ventajas, tanto para las empresas como para consumidores, que supondría la transformación digital en sectores como las finanzas, la manufactura, la educación, la salud, entre otros.

En la industria alimentaria podría ser de utilidad como parte de la gestión de la cadena de suministro permitiendo hacer un seguimiento de los productos desde su fabricación hasta su distribución final, aislando así problemas de forma fácil y eficiente. En el sector sanitario podría llegar a proporcionar un registro absoluto de datos que permitirían abordar investigaciones científicas, además de dar la posibilidad de optimizar la privacidad del historial de los pacientes a la vez que mantener la información unificada mejorando su administración.

[40] MALDONADO, J., (2021, 1 marzo). Los NFT revolucionan la industria de la música: 3LAU recauda más de $11 millones. OBSERVATORIO BLOCKCHAIN. [consultado 24/01/2022]. Disponible en: https://observatorioBlockchain.com/nft/los-nft-revolucionan-la-industria-de-la-musica-3lau-recauda-mas-de-11-millones/

Respecto al sector energético controlado actualmente por grandes compañías, cada vez más hogares se lanzan a la producción de su propia electricidad con energías renovables y a través de blockchain se podría crear una red entre casas para la compra y venta de energía, convirtiéndola en un activo. Se conocen ya iniciativas como la Pylon Network o Power Ledger.

En el sector inmobiliario, ya se ha mencionado anteriormente, aunque de forma breve su utilidad a través de los contratos inteligentes, permitiendo establecer las condiciones del contrato y almacenarlo en la blockchain para su posterior ejecución automática.

Finalmente, la aplicación de esta tecnología para la creación de identidades digitales asociadas a una persona es unas propuestas más novedosas que se plantean. Esto dará posibilidad a operar en diferentes plataformas, evitando así la violación de datos y la documentación física.

IX. CONCLUSIONES

PRIMERA. La tecnología blockchain lleva desarrollándose varios años desde su aplicación en Bitcoin, pero no es hasta 2020 cuando logra su auge sobre todo captando la atención de aquellos más interesados en las nuevas tecnologías, gracias entre otras cosas al tiempo libre que originó el confinamiento debido a la pandemia sobrevenida en la que nuestra sociedad se vio inmersa.

SEGUNDA. La blockchain o cadena de bloques responde a una base de datos de carácter descentralizado que surge de la implementación de dos elementos: la tecnología de registro distribuido, ya mencionada, DLT y la encriptación. Características como la inmutabilidad de la red, la trazabilidad, la agilidad que permite en las transacciones y la incensurabilidad justifican la cantidad de usos de esta en ámbitos muy diversos como las finanzas, la educación, la salud o la energía entre otros.

Sin duda esta tecnología nos abre las puertas a un sinfín de posibilidades y aplicaciones más allá de las criptomonedas que pueden provocar una disrupción en el sistema tradicional a nivel económico, pero también legal.

TERCERA. En España no hay regulación específica, se aborda a través de la normativa relativa a la prevención y blanqueo de capitales que establece una reglamentación básica que deja múltiples frentes abiertos. A nivel comunitario ocurría similar, pero desde 2018 se trabaja en la creación de un marco europeo común para regular el mercado de las criptomonedas, lo que se conoce como la propuesta del Reglamento MiCA (siglas en inglés de Markets in Crypto-Assets), aunque su implementación no se prevé hasta 2024.

CUARTA. Actualmente 4,5 millones de españoles invierten en criptomonedas y mientras unos pocos se hacen millonarios, otros pierden todo su capital, por lo que es importante destacar no sólo las ventajas de esta innovación, sino también los riesgos.

La extrema volatilidad, la complejidad de esta tecnología y la falta de transparencia son algunas de las características sobre las que advierte la CNMV, además de la falta de consideración como medio de pago al no cumplir adecuadamente las funciones de unidad de cuenta y depósito de valor, y la inexistencia respaldo de un banco central u otra autoridad pública, así como de un mecanismo de protección.

QUINTA. En resumen, debemos ser conscientes de las múltiples formas que existen de aplicar la blockchain y las oportunidades que esto va a suponer, por ello considero que es clave solventar el desconocimiento de la población y la falta de regulación, pero sin limitar el crecimiento de este nuevo mercado.

BIBLIOGRAFÍA

LIBROS

FERRUZ AGUDO, L. y RIVAS, J. (2021). *Fraude Codicia Ignorancia: Las burbujas financieras en los mercados*. España: Independently Publisher

PREUKSCHAT, A., *Blockchain: La revolución industrial de Internet*, 2019, Ediciones Gestion 2000, Barcelona

TAPSCOTT. A y TAPSCOTT. D, *Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world*, 2016, Penguin Random House

REVISTAS Y ARTICULOS ELECTRÓNICOS

GANNE, E. «Can Blockchain revolutionize international trade?» WORLD TRADE ORGANIZATION Publications [revista electrónica], 2018 [consultado 28/01/2022]. Disponible en: https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf

FERNANDEZ DE LIS, S. y GOUVEIA, O. «Monedas digitales emitidas por bancos centrales:
características, opciones, ventajas y desventajas». BBVA RESEARCH [revista electrónica], 2019, nº19/03 [consultada 10/01/2022]. Disponible en: https://www.bbvaresearch.com/wp-content/uploads/2019/03/WP_Monedas-digitales-emitidas-por-bancos-centrales-ICO.pdf

NAKAMOTO, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* BITCOIN.ES [consultado 28/01/2021]. Disponible en: https://bitcoin.org/bitcoin.pdf

RECURSOS ELECTRÓNICOS

BELINCHÓN, F. (2021, 1 abril). Riesgos de las divisas virtuales para los particulares. EL PAÍS, Cinco Días [consultado 13/02/2022]. Disponible en: https://cincodias.elpais.com/cincodias/2021/04/01/mercados/1617278607_020694.html

SOLERA, S. (2021). *Blockchain: qué es, cómo funciona y los usos más comunes*. OCCAM. [consultado 10/11/2021]. Disponible en: https://www.occamagenciadigital.com/blog/Blockchain-que-es-como-funciona

West, P. (2018, 19 febrero). *Is distributed ledger technology the answer? Open Innovation Team*. OPENINNOVATION [consultado 17/11/2021]. Disponible en: https://openinnovation.blog.gov.uk/2018/02/19/is-distributed-ledger-technology-the-answer/

Hoff, T. (2018, 10 febrero). *La compleja infraestructura detrás de Netflix: ¿qué pasa cuando le das al «play»?* XATAKA. [consultado 28/11/2021]. Disponible en: https://www.xataka.com/streaming/la-compleja-infraestructura-detras-de-netflix-que-pasa-cuando-le-das-al-play

Fernández, Y. (2021, 8 febrero). *BitTorrent: qué es y cómo funcionan los torrents.* XATAKA. [consultado 01/12/2021]. Disponible en: https://www.xataka.com/basics/bittorrent-que-como-funcionan-torrents

Carisio, E. (2019, 26 junio). *Para qué sirve la criptografía de clave pública y privada*. MDCLOUD. [cponsultado 15/12/2021]. Disponible en: https://blog.mdcloud.es/para-que-sirve-la-criptografia-de-clave-publica-y-privada/

SUBHASISH, S. (2020, 4 julio). Know about the Caesar Cipher, one of the earliest known and simplest ciphers. IBM Community- Z Security [consultado 17/11/2021]. Disponible en: https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/04/caesar-cipher

Blockchain 101. (2020, 11 enero). *The cryptography used in Blockchain*. APRENDE BLOCKCHAIN. [consultado 17/12/2021]. Disponible en: https://aprendeBlockchain.wordpress.com/Blockchain-101-ii/

Blockchain 101. (2018, 18 febrero). *Conceptos de seguridad y criptografía en Blockchain*. APRENDE BLOCKCHAIN. [consultado 18/12/2021]. Disponible en: https://aprendeBlockchain.wordpress.com/fundamentos-tecnicos-de-Blockchain/fundamentos-basicos-de-criptografia-en-Blockchain/

Rodriguez, N. (2019, 14 enero). *6 Características clave de la tecnología Blockchain que debes conocer!*. 101 BLOCKCHAINS. [consultado 12/12/2021]. Disponible en: https://101Blockchains.com/es/caracteristicas-tecnologia-Blockchain/

FRANKENFIELD, J., (2021, 22 julio). *What Is Proof of Work (PoW)?* INVESTOPEDIA. [consultado 17/12/2021]. Disponible en: https://www.investopedia.com/terms/p/proof-work.asp

CoinTelegraph. (2020, 22 abril). *¿Qué es el nonce? Un número vital en Bitcoin. Investing.com* Español. https://es.investing.com/news/cryptocurrency-news/que-es-el-nonce-un-numero-vital-en-Bitcoin-1991973

Nieto, A. (2018). *El número de Bitcoins es finito, no podrá haber más de 21 millones: ¿qué se espera que suceda entonces?*. XATAKA. [consultado 17/12/2021]. Disponible en: https://www.xataka.com/criptomonedas/el-numero-de-Bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces

YOUNG, M. (2021, 13 enero). ¿Cuántos de los 21 millones de Bitcoin quedan?. BEINCRYPTO. [consultado 13/02/2021]. Disponible en: https://es.beincrypto.com/cuantos-21-millones-bitcoin-btc-quedan/

ROSEN, P. (2021, 15 diciembre). *El 90% de los bitcoin ya han sido minados, pero el 10% restante tardará 120 años en llegar al mercado.* BUSINESS INSIDER. [consultado 13/02/2022]. Disponible en: https://www.businessinsider.es/cuantos-bitcoins-han-minado-ya-980561

MUÑOZ CABANES, A. (2021, 4 enero). *¿Qué diferencias hay entre una moneda digital y una criptomoneda?*. BBVA Communications. [consultado 22/12/2021]. Disponible en: https://www.bbva.com/es/que-diferencias-hay-entre-una-moneda-digital-y-una-criptomoneda/

iProUP (2021, 13 diciembre). *Sólo resta el 10% de Bitcoin por minar: ¿cuándo se obtendrá el último BTC?*. ECONOMÍA DIGITAL iProUP [consultado 20/01/2022]. Disponible en: https://www.iproup.com/economia-digital/28169-bitcoin-cuantas-unidades-quedan-aun-por-minar

E. (2021, 9 agosto). *¿Qué diferencias hay entre una moneda digital y una criptomoneda?* BBVA RESEARCH. [consultado 16/11/2021]. Disponible en: https://www.bbva.com/es/que-diferencias-hay-entre-una-moneda-digital-y-una-criptomoneda/

ZAVALA, A., (2018). Blockchain: qué es un token y los usos que puede llegar a tener. EXPANSIVE [consultado 24/12/2021]. Disponible en: https://blog.expansive.mx/2018/03/08/Blockchain-que-es-un-token-y-los-usos-que-puede-llegar-a-tener/

MARTESANZ, V., (2021, 9 diciembre). *Qué es una wallet de criptomonedas, qué tipos hay y cómo elegir una*. FINECT [consultado 7/01/2022]. Disponible en: https://www.finect.com/usuario/vanesamatesanz/articulos/wallet-criptomonedas-que-es-tipos-como-elegir

PANETTA, F. (2021, 19 noviembre). *The ECB's case for central bank digital currencies*. ECB.EUROPA [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog211119~fda94a3f84.es.html

EUROPAPRESS (2022, 11 de enero). *El FMI alerta de la capacidad de los criptoactivos para desestabilizar los mercados e insta a regularlos.* Economía - EUROPAPRESS [consultado 13/02/2022]. Disponible en: https://www.europapress.es/economia/finanzas-00340/noticia-fmi-alerta-capacidad-criptoactivos-desestabilizar-mercados-insta-regularlos-20220111174039.html

ECB. (2021, 14 julio). *El Eurosistema pone en marcha el proyecto de un euro digital*. ECB.EUROPA Nota de Prensa. [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.es.html

PANETTA, F. (2021). *Un euro digital*. EBC. EUROPA [consultado 13/02/2021]. Disponible en: https://www.ecb.europa.eu/paym/digital_euro/html/index.es.html

SAEZ HURTADO, J. (2021, 8 agosto). Las 10 criptodivisas (o criptomonedas) con más futuro. IEBSCHOOL [consultado 18/01/2022]. Disponible en: https://www.iebschool.com/blog/criptodivisas-criptomonedas-invertir-finanzas/#:~:text=Hoy%20en%20d%C3%ADa%20existen%20m%C3%A1s,y%20la%20filosof%C3%ADa%20que%20utilizan

CNMV (2021, 9 febrero). Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión. CNMV y BANCO DE ESPAÑA. [consultado 13/01/2022]. Disponible en: https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D

TOKENIZA (2020, 14 abril). Cómo es el proceso de Tokenización de un activo inmobiliario. TOKENIZA-Activos en Blockchain [consultado 16/01/2022]. Disponible en: https://www.tokeniza.es/como-es-el-proceso-de-tokenizacion-de-un-activo/

SOLERA, S. (2021, 21 septiembre). *¿Cómo tokenizar un inmueble?* OCCAM. [consultado 16/01/2022]. Disponible en: https://www.occamagenciadigital.com/blog/como-tokenizar-un-inmueble

RAEVENLORD, (2021, 14 mayo). *Binance, World's Largest Crypto Exchange, Reportedly Under Investigation by DoJ, IRS.* TECHPOWERUP. [consultado 13/02/2022]. Disponible en: https://www.techpowerup.com/282228/binance-worlds-largest-crypto-exchange-reportedly-under-investigation-by-doj-irs

RUS ARIAS, E. (2021, 5 octubre). Exchange de criptomonedas. ECONOMIPEDIA.COM. [consultado 17/12/2021]. Disponible en: https://economipedia.com/definiciones/exchange-de-criptomonedas.html#:~:text=Tenemos%20dos%20categor%C3%ADas%20de%20exchange,otras%20las%20descentralizadas%20(DEX).

WEHOLDERS (2021, 7 junio). COMPARATIVA: Los 3 MEJORES EXCHANGES de CRIPTOMONEDAS [+1 por si eres EMPRESA]. WEHOLDERS- Inversión en bolsa. [consultado 26/01/2022]. Disponible en: https://weholders.com/comparativa-los-3-mejores-exchanges-de-criptomonedas-1-por-si-eres-empresa/#Exchanges_P2P

RAEVENLORD, (2021, 14 mayo). *Binance, World's Largest Crypto Exchange, Reportedly Under Investigation by DoJ, IRS.* TECHPOWERUP. [consultado 13/02/2022]. Disponible en: https://www.techpowerup.com/282228/binance-worlds-largest-crypto-exchange-reportedly-under-investigation-by-doj-irs