Universidad de Oviedo

FACULTAD DE ECONOMÍA Y EMPRESA

GRADO EN CONTABILIDAD Y FINANZAS

2021/2022

TRABAJO FIN DE GRADO

BLOCKCHAIN: MÁS ALLÁ DE LAS CRIPTOMONEDAS

DANIEL CORGO SUÁREZ

Oviedo, 1 de julio de 2022

BLOCKCHAIN: MÁS ALLÁ DE LAS CRIPTOMONEDAS

Daniel Corgo Suárez, Grado en Contabilidad y Finanzas, Facultad de Economía y Empresa, Universidad de Oviedo, España (2022).

Email: uo247389@uniovi.es

TÍTULO EN ESPAÑOL: *Blockchain*: más allá de las criptomonedas

RESUMEN EN ESPAÑOL: Este trabajo de fin de grado se centra en la tecnología *blockchain*, en el que se tratará de explicar la naturaleza, el funcionamiento y cuáles son las aplicaciones de mayor importancia de esta tecnología. También se dotará de una introducción a los elementos que están estrechamente relacionados con la *blockchain*, como los contratos inteligentes, las aplicaciones descentralizadas o las conocidas criptomonedas, explicando sus funciones y crecimiento desde su aparición en 2009 con el *Bitcoin*. A la hora de proporcionar una visión general del funcionamiento, de su importancia en la actualidad y posible importancia futura, es imperativo destacar la importancia de las criptomonedas, así como subrayar tanto sus ventajas como desventajas económicas. También se explicarán los conocidos *tokens* no fungibles para entender tanto su funcionamiento como sus posibles usos.

Palabras clave: *Blockchain*, criptomonedas, *Bitcoin*, *tokens*.

TÍTULO EN INGLÉS: Blockchain: beyond cryptocurrencies

ABSTRACT: This final degree project focuses on blockchain technology, in which we will try to explain the nature, functioning and most important applications of this technology. It will also provide an introduction to the elements closely related to blockchain, such as smart contracts, decentralized applications or the well-known cryptocurrencies, explaining their functions and growth since their appearance in 2009 with Bitcoin. To provide an overview of how they work and their current and possible future importance, it is imperative to highlight the importance of cryptocurrencies and underline their economic advantages and disadvantages. The well-known non-fungible tokens (NFTs) will also be explained to understand their functioning and possible uses.

Keywords: Blockchain, crytocurrencies, Bitcoin, tokens.

ÍNDICE

1. INTRODUCCIÓN

La tecnología *blockchain* o cadena de bloques es una de las grandes innovaciones del presente siglo, debido a su contribución en sectores como el financiero o el público. La primera aproximación a la *blockchain* fue en 1991, cuando Stuart Haber y W. Scott Stornetta trabajaron en una cadena de bloques protegida mediante la criptografía en la que las marcas de tiempo de los documentos eran inmutables (Whitaker, 2018).

Al año siguiente actualizaron su sistema incorporando los árboles de *Merkle* o árbol *Hash*, que como su nombre indica, se trata de una estructura de datos en árbol, normalmente binarios, mejorando así la eficiencia y permitiendo que cada bloque pudiese incorporar más documentos. A pesar de estos avances, la *blockchain* no adquirió gran importancia hasta el 2008, gracias al trabajo de una persona o grupo de personas, cuya identidad se desconoce, bajo el seudónimo de Satoshi Nakamoto, creador del *Bitcoin*, siendo esta la primera aplicación de la tecnología de registro digital (Delfabro *et al*., 2021).

El primer informe de Satoshi Nakamoto sobre esta tecnología vio la luz en 2009, enfatizando la importancia de la descentralización, que permite escapar del control por parte de los gobiernos de cada país. Con esta idea surgen las criptomonedas, que utilizando la tecnología *blockchain* se entienden como una nueva forma de dinero (Nakamoto, 2008).

Desde su origen, las criptomonedas crean una gran expectativa. Esto queda claramente patente en el gran número de criptomonedas existentes, calculado en más de 10.000 tipos desde el comienzo del *Bitcoin*, aunque no todas siguen existiendo en la actualidad (Sáez, 2022). Este innovador activo de inversión, que también puede funcionar como moneda de cambio en determinadas transacciones, ha traído con su irrupción un mundo entero a su alrededor, creando desde especialistas en su tecnología hasta cambios importantes en la manera de gestionar y de almacenar inmensas cantidades de información de manera segura y veraz. El mantenerse al día de las novedades en este ámbito se ha convertido en una tarea complicada desde su inicio, debido a la gran cantidad de información publicada a diario a su respecto, lo que complica que cualquier información mantenga su vigencia en un largo periodo de tiempo.

La capacidad de esta tecnología para registrar cualquier tipo de transacción *peer-to-peer* (red entre pares) de una forma segura, eficiente, verificable e inmutable da como resultado la posibilidad de ser aplicada a otras tareas no financieras, como puede ser la contabilidad, pudiendo resolver problemas de alta magnitud como la piratería musical (Puentes, 2019). También puede ser muy útil en otros ámbitos como la transmisión de votos, el control sobre el origen de los productos u otros tipos de sectores públicos, ya que permite un control exhaustivo de forma segura y con total transparencia (García, 2018).

En este documento se pretende acercar al lector a la tecnología de la *blockchain* y su potencial, destacando la importancia de las criptomonedas dentro de esta tecnología, cuya irrupción hace posible la transformación de toda práctica social en la que sea importante corroborar la veracidad e identidad de un documento.

La organización de este trabajo de fin de grado se basa en una primera parte, en la que se lleva a cabo el desarrollo de la *blockchain*, desde sus bases hasta las aplicaciones descentralizadas. En segundo lugar, se realiza una explicación detallada de las criptomonedas, haciendo especial mención a las de mayor importancia, así como sus ventajas e inconvenientes y su actual situación. En tercer lugar, se resalta la utilización de los *tokens* no fungibles en la actualidad. Finalmente, se exponen las conclusiones del trabajo.

2. *BLOCKCHAIN*

La tecnología *blockchain* o cadena de bloques es un nuevo paradigma que tiene como objetivo principal fomentar la red descentralizada frente al mecanismo centralizado convencional. La función de descentralización es la base de esta tecnología, que permite que las criptomonedas sean teóricamente inmunes a las clásicas formas de gobierno y control bancario, además de eliminar la necesidad de cualquier tercero o mediador (Sakiz *et al*., 2018). Por lo tanto, se puede definir como una red distribuida, que se puede utilizar como un libro de contabilidad digital, así como un mecanismo que permite la transferencia segura de activos sin una autoridad central, facilitando el intercambio digital de unidades de valor (Aggarwal and Kumar, 2020).

La primera forma de tecnología *blockchain* mantenida por consenso anónimo fue *Bitcoin*, creada por Satoshi Nakamoto. Esta permitía a los usuarios transferir la moneda de forma segura sin un regulador centralizado. Desde entonces, se han propuesto varias plataformas de desarrollo basadas en la *blockchain* que ofrecen la capacidad de usar contratos inteligentes para ejecutar automáticamente acciones. Entre ellos, destacan *Ethereum* e *Hyperledger Fabric* (Sakiz *et al*., 2018)

Con el fin de facilitar la comprensión de este trabajo de fin de grado, es necesario definir una serie de conceptos que se irán mencionando a lo largo del desarrollo, debido a su estrecha relación con la *blockchain*. Entre ellos se encuentran:

- **Nodo**: se refiere al usuario u ordenado. Cada uno de ellos tiene una copia original de la *blockchain* y, por lo tanto, son capaces de determinar si las operaciones planteadas por el resto de los usuarios de la red pueden realizarse o no (Porxas y Conejero, 2018).

- **Protocolo**: conjunto básico de reglas o algoritmos cuya función es permitir el intercambio de información entre los nodos. Es decir, establecen la estructura de la *blockchain*. Incorporan los incentivos que consiguen que las partes actúen de forma honesta (Gómez, 2018).

- **Bloques**: es el lugar donde se crea una copia exacta de la información. Al conseguir que cada uno de los nodos incluidos en la red verifiquen y confirmen la información se crea el nuevo bloque, con el *hash* que le corresponda, y se añade este a la cadena sin la intervención de un tercero. Estos bloques de transacciones suelen ser publicados a intervalos de diez minutos en el libro contable (Simoes, 2022).

- ***Hash***: es un algoritmo matemático que tiene la capacidad de transformar cualquier bloque de datos en otra serie de datos nueva con una longitud fija, independientemente de cuál sea la longitud de los datos de entrada (Porxas y Conejero, 2018).

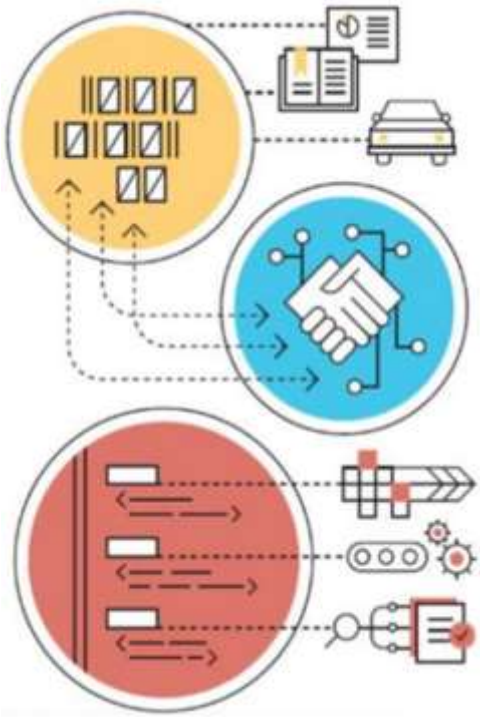
- **Billetera (*wallet*)**: se parece a la clásica cuenta corriente bancaria. Una de las virtudes de esta cartera virtual es el control que posee el usuario sobre sus criptodivisas, sin depender de ninguna empresa externa. De este modo, los fondos de cada cliente no podrán ser retenidos o congelados por ninguna autoridad. Existen diferentes tipos según sean *online* o físicos, siendo más seguros estos últimos (Gómez, 2018).

Cabe señalar que esta tecnología ha sido ideada principalmente para el sector financiero. No obstante, otras industrias también pueden utilizarla (Piscini *et al*., 2017), como son los servicios sanitarios (compartir ensayos clínicos en tiempo real), sector público (mayor seguridad y transparencia de la votación en las elecciones públicas), energía y recursos (gestión y registro de transacciones de petróleo y gas y conexión de proveedores, transportistas y contratistas para mejorar los procesos de la cadena de

suministro), medios tecnológicos y telecomunicaciones (almacenamiento de *hash* criptográfico de música original) y productos de consumo e industriales (mejora de la trazabilidad).

2.1. BASES DE LA *BLOCKCHAIN*

En la tecnología *blockchain* los ordenadores conectados a la red actúan como nodos que registran la información dentro de la cadena de bloques mediante un proceso criptográfico (Khan *et al*., 2021), probando de esta manera cuál ha sido el ordenador que ha resuelto la operación matemática de manera correcta. El consenso es muy importante en esta red (Trautman and Molesky, 2018), impidiendo así la falsificación de información, ya que para realizar esta tarea deberían de estar de acuerdo más de la mitad de los ordenadores conectados a la red, al mismo tiempo y sin posibilidad de coordinación entre sí. Por ello, no se permite la eliminación de ninguna información dentro de la red ni su modificación. Esto se realiza sin comprometer de ninguna manera la privacidad de los usuarios, registrando el momento de las operaciones y si estas han sido correctas, pero no incluye el tipo de evento o las partes involucradas en él (Khan *et al*., 2021).



1. Almacenamiento de registros digitales
Blockchain permite un control sin precedentes de la información mediante registros seguros, auditables e inmutables de no solo transacciones, sino de representaciones digitales de activos físicos.

2. Intercambio de activos digitales
Los usuarios pueden emitir nuevos activos y transferir la propiedad en tiempo real sin bancos, bolsas de valores o procesadores de pago.

3. Ejecución de contratos inteligentes
El auto-gobierno de los contratos simplifica y automatiza procesos de negocio prolongados e ineficientes.

Reglas de juego. Los términos y condiciones son registrados en el código de contrato.

Implementación. La red compartida automáticamente ejecuta el contrato y monitoriza el cumplimiento.

Verificación. Los resultados son válidos instantáneamente sin un tercero.

Figura 1. Niveles de la *blockchain* (Piscini *et al*., 2017).

La tecnología *blockchain* ha facilitado la aportación de muchos beneficios en la economía mundial, ya que permite el almacenamiento de registros digitales, intercambio de activos digitales entre distintos miembros sin necesidad de un intermediario y la ejecución de contratos inteligentes. Esto es lo que se conoce como los tres niveles de la *blockchain* (Figura 1).

2.2. TIPOS DE *BLOCKCHAIN*

En la actualidad hay diferentes tipos de *blockchain* con sus características específicas (Tabla 1; Zemlianskaia, 2017; Parrondo, 2018), entre los que destacan:

- ***Blockchain* pública**. Se trata del primer tipo de *blockchain*, refiriéndose a las que tienen un acceso público a través de internet, como pueden ser *Bitcoin* o *Ethereum* (Trautman and Molesky, 2018). En esta *blockchain* se mantienen los datos abiertos al público general, de forma que cualquiera pueda acceder a ellos libremente. Para ello poseen unas grandes medidas de seguridad que no permiten alterar su funcionamiento de forma maliciosa. Una de sus principales ventajas es la no existencia de entidades centralizadas, es decir, ninguna autoridad central regula su funcionamiento, por ello se suelen considerar como totalmente descentralizadas (Woonkly, 2022).

- ***Blockchain* privada**. Aquí una autoridad central decide y atribuye el derecho a participar en las operaciones de escritura o lectura de la *blockchain*. Esto hace que no todos los usuarios tengan acceso a su información, si no aquellos acreditados por dicha autoridad central (Trautman and Molesky, 2018). Sus posibles aplicaciones incluyen desde la administración de bases de datos hasta las auditorías internas realizadas para una sola empresa (Deloitte, 2022). El mayor ejemplo es el proyecto de la Fundación *Linux* llamado *Hyperledger Fabric*, formado por decenas de miembros cuyo objetivo es crear una plataforma común para estas *blockchain* privadas (Trautman and Molesky, 2018).

- ***Blockchain* de consorcio**. Es una fusión entre los tipos de *blockchain* previamente mencionados. Las empresas líderes en el sector financiero y bancario crean estos consorcios. Estas empresas están conectadas a la *blockchain* y son las responsables de validar cada bloque, para lo cual es necesario un consenso entre ellas (Zemlianskaia, 2017).

Tabla 1. Diferencias entre las cadenas de bloques privadas y públicas (Zemlianskaia, 2017).

	***Blockchain* pública**	***Blockchain* privada**
Acceso	Lectura y escritura abiertas	Lectura y escritura bajo permiso
Velocidad	Lenta	Rápida
Seguridad	Red abierta	Usuarios aprobados
Identificación	Anónimas o seudoanónimas	Conocidas
Activos	Nativos	Cualquier activo

2.3. MECANISMOS DE CONSENSO

El mecanismo de consenso es la clave de la tecnología *blockchain*. El consenso en una red de cadena de bloques se refiere al proceso en el que los nodos distribuidos acuerdan el historial y el estado final de los datos en el libro mayor, generalmente denominado consenso distribuido. Dado que todos los participantes en la red tienen los datos, también pueden ser parte de la toma de decisiones. Cada nuevo bloque que se agrega a la *blockchain* debe pactarse de acuerdo con el protocolo definido para que la replicación se realice de manera uniforme. Se han desarrollado numerosos algoritmos de consenso, haciendo especial mención a los dos siguientes (Trautman and Molesky, 2018):

- ***Proof Of Work* (PoW)**: fue el primer protocolo consenso descentralizado propuesto por Nakamoto para lograr la consistencia y seguridad en la red *Bitcoin*. En *Bitcoin*, la transferencia de divisas se produce de forma completamente

descentralizada, por lo que se requiere un consenso para la autenticación y la validez de los bloques. Los nodos de la red *Bitcoin* compiten para calcular el valor *hash* del siguiente bloque, que se supone que es menor que un valor objetivo que varía dinámicamente, determinado por la regla de consenso. Los nodos que logran la solución esperan la confirmación de otros nodos antes de agregar el bloque a la cadena de bloques existente. Se puede generar más de un bloque válido si varios nodos encuentran una solución adecuada que provoca una bifurcación (rama) temporal en la red. En tales casos, todos ellos son aceptables y los nodos más cercanos a los mineros, aceptan la solución que reciben y la envían a otros pares. El conflicto en una etapa posterior se evita aceptando la versión más larga de la cadena disponible en cualquier momento.

- ***Proof Of Stake*** **(PoS)**: este protocolo fue propuesto para superar las desventajas del consumo excesivo de energía mediante la PoW en *Bitcoin*. *Ethereum* utiliza la PoS para superar el consenso. En lugar de invertir en recursos que puedan realizar cálculos rigurosos para cálculos *hash* en la PoW, la PoS propone comprar criptomonedas y utilizarlas como participación en la red. Esta apuesta es directamente proporcional a la posibilidad de convertirse en el validador del bloque. Para llegar a un consenso, el validador de bloques se selecciona aleatoriamente y no está predeterminado. Los nodos que producen bloques válidos obtienen incentivos, pero, si su bloque no está incluido en la cadena existente, también pierden parte de su participación.

2.4. *SMART CONTRACTS*

En los últimos años, el rápido desarrollo de la tecnología *blockchain* y las criptomonedas ha influido en la industria financiera al crear una nueva criptoeconomía. Las aplicaciones descentralizadas de última generación que no involucran un intermediario han surgido gracias a la aparición de los *smart contracts* (contratos inteligentes). Estos son protocolos informáticos diseñados para facilitar, verificar y hacer cumplir automáticamente la negociación y el acuerdo entre las múltiples partes no confiables (Khan *et al*., 2021; Nadler *et al*., 2021; Trautman and Molesky, 2018).

Los *smart contracts* brindan una automatización de la red y la capacidad de convertir contratos en papel en contratos digitales, permitiendo a los usuarios codificar sus acuerdos y relaciones de confianza al proporcionar transacciones automatizadas sin la supervisión de una autoridad central (Parrondo, 2018). Para evitar la manipulación de contratos, estos *smart contracts* se copian en cada nodo de la red de la *blockchain*. Las cláusulas del contrato escritas en los programas computacionales se ejecutan automáticamente cuando se cumplen las condiciones predefinidas. Las ventajas que tienen los *smart contracts* en comparación con los contratos convencionales se pueden resumir en las siguientes (Legerén-Molina, 2018):

- **Reducción de riesgos**. Debido a la inmutabilidad de las cadenas de bloques, los contratos inteligentes no pueden modificarse arbitrariamente una vez que se emiten. Además, todas las transacciones que se almacenan y duplican en todo el sistema de cadena de bloques son rastreables y auditables. Como resultado, los fraudes financieros pueden mitigarse en gran medida.
- **Reducción de costes de administración y servicios**. Las *blockchain* aseguran la confianza de todo el sistema mediante mecanismos de consenso distribuidos sin pasar por una autorización central o un mediador. Los contratos inteligentes almacenados en las *blockchain* se pueden activar automáticamente de forma descentralizada. En consecuencia, los costes de administración y servicios debidos a la intervención de terceros pueden ahorrarse significativamente.

- **Mejorar la eficiencia de los procesos de negocio**. La eliminación del intermediario puede mejorar significativamente la eficiencia del proceso comercial. La liquidación financiera se completará automáticamente de manera *peer-to-peer* una vez que se cumpla la condición predefinida (por ejemplo, el comprador confirma la recepción de los productos). Como resultado, el tiempo de respuesta se puede reducir considerablemente.

Aunque los *smart contracts* tienen un gran potencial para remodelar procedimientos comerciales convencionales, hay una serie de desafíos todavía por resolver. Por ejemplo, incluso si las cadenas de bloques pueden garantizar cierto anonimato de las partes del contrato, es posible que no se preserve la privacidad de la ejecución del contrato en su totalidad, ya que todas las transacciones están disponibles a nivel mundial. Además, es un desafío garantizar la corrección de los contratos inteligentes debido a las vulnerabilidades de los programas informáticos (Trautman and Molesky, 2018).

2.4.1. Fases del *smart contract*

El ciclo de vida de un contrato inteligente consta de cuatro fases principales (Zheng *et al*., 2019): creación, implementación, ejecución y finalización, las cuales se detallan a continuación:

1. **Creación**. Las partes involucradas negocian primero sobre las obligaciones, derechos y prohibiciones de los contratos. Los abogados o consejeros ayudarán a las distintas partes a redactar un acuerdo contractual inicial, para que los ingenieros de *software* lo conviertan en un *smart contract* con lenguaje informático propio. La conversión del contrato inteligente se compone de diseño, implementación y validación.

2. **Implementación**. Una vez validados, se pueden implementar en plataformas sobre cadenas de bloques. Como se ha dicho con anterioridad, los contratos almacenados en dichas cadenas no se pueden modificar debido a la inmutabilidad de las *blockchain*. Cualquier modificación requiere la creación de un nuevo contrato. Una vez implementados en las cadenas, todas las partes pueden acceder a ellos a través de las *blockchain*. Además, los activos digitales de las partes involucradas en el *smart contract* se bloquean congelando las billeteras digitales correspondientes. Por ejemplo, se bloquean las transferencias de monedas (entrantes o salientes) en las billeteras relevantes para el contrato. Mientras tanto, las partes pueden ser identificadas por sus carteras digitales.

3. **Ejecución**. En esta fase las cláusulas contractuales son objeto de seguimiento y evaluación. Una vez cumplidas las condiciones, se ejecutan automáticamente los trámites o funciones contractuales. Cabe señalar que un contrato inteligente consta de una serie de declaraciones con conexiones lógicas. Cuando se activa una condición, se ejecuta la instrucción correspondiente, por lo que los mineros ejecutarán y validarán la transacción en las *blockchain*. Las transacciones comprometidas y los estados actualizados se almacenarán en las cadenas de bloques a partir de este momento.

4. **Finalización**. Después de ejecutar un contrato inteligente, se actualizan los nuevos estados de todas las partes involucradas. De esta forma, las transacciones durante la ejecución y los estados actualizados, se almacenarán en la *blockchain*. Mientras tanto, los activos digitales se transfieren de una parte a otra (por ejemplo, la transferencia de dinero del comprador al proveedor). Por consiguiente, se desbloquean los activos digitales de las partes involucradas.

2.5. APLICACIONES DESCENTRALIZADAS Y FINANZAS DESCENTRALIZADAS

Las aplicaciones descentralizadas (*Descentralized Applications*, DApps) ofrecen servicios similares a las aplicaciones típicas, diferenciándose en la utilización de la tecnología *blockchain* para ofrecer un mayor control sobre los datos personales al no ser necesaria la participación de intermediarios centralizados para que los administren, aumentando así la protección sobre las finanzas (Fernández, 2022). En la actualidad, hay una verdadera industria de aplicaciones descentralizadas dentro de la *blockchain*, desde finanzas hasta juegos o coleccionismo de arte. La mayoría de este tipo de aplicaciones están construidas con *Ethereum* y todas ellas utilizan la tecnología *blockchain* (Fernández, 2022). Su utilidad se basa en cadenas de bloques que procesan los datos y en ejecutar las transacciones mediante los *smart contracts.* Las aplicaciones descentralizadas se pueden dividir en tres grupos, aplicaciones financieras (*Descentralized Finance*, DeFi), aplicaciones semifinancieras (con datos fuera de la cadena de bloques) y otras aplicaciones (Fernández, 2022).

Las DeFi son las que tienen mayor importancia y las que más nos incumben dentro de las aplicaciones descentralizadas. Son las aplicaciones que ofrecen la posibilidad de utilizar sistemas financieros sin depender de entidades centralizadas. Esto se produce gracias a los *smart contracts* y las DApps, quedando así grabadas todas las operaciones en la *blockchain* de manera inalterable y permanente (Segura, 2021).

El nacimiento de las DeFi surgió dentro de la *blockchain* de *Ethereum*, siendo este posible gracias a los contratos inteligentes flexibles que incluye esta cadena de bloques (Segura, 2021). El objetivo de estas finanzas es la construcción de un mejor panorama financiero posibilitado con la llegada de internet y de la tecnología *blockchain*, destacando la importancia de los siguientes aspectos (Lau *et al*.,2020):

- **Accesibilidad**. Posibilitan el acceso a los servicios financieros sin barreras geográficas, llegando así a cualquier parte del mundo, algo que es más complicado para las finanzas tradicionales.
- **Solución a problemas financieros mundiales**. La quiebra de algunos bancos en la crisis financiera de 2008 provocó la pérdida de su fortuna a muchas personas, siendo estas nuevas tecnologías un método para protegerse frente a problemas de este tipo.
- **Evitar censura y restricciones**. La gran cantidad de medidas regulatorias existentes en el sector financiero tradicional no se dan en las DeFi, facilitando, por ejemplo, las transacciones entre personas de diferentes países. La falta de censura y de control también tiene su parte negativa, favoreciendo las operaciones ilegales ya que la privacidad del usuario es mucho mayor.
- **Mejora de los sistemas de pago**. Las criptomonedas sustentadas en esta tecnología permiten una mayor velocidad al realizar operaciones, con mayor privacidad y, por lo general, con comisiones más bajas que las cobradas por las instituciones bancarias (Borrega, 2021).

3. CRIPTOMONEDAS

La revolución digital trajo consigo la inevitable evolución de la moneda. La idea de la criptomoneda surgió por primera vez en 1983, cuando el criptógrafo estadounidense, David Chaum, creó la primera forma de criptomoneda denominada *ECash* y después desarrolló un sistema de pago electrónico que era casi imposible de rastrear por el sistema bancario o las agencias gubernamentales (Rice, 2019). Durante los siguientes años, surgieron en el mercado múltiples formas financieras de criptomonedas

mejoradas, como *Bit Gold*, considerada la precursora de *Bitcoin*. Esta fue creada por Nick Szabo, quien utilizó como base el trabajo de Chaum, sin embargo, no pudo resolver el problema del doble gasto sin el uso de una autoridad central. Por ello, una década más tarde, una persona o grupo de personas, bajo el seudónimo de Satoshi Nakamoto, crearon el *Bitcoin* en 2009 (Aziz, 2019), cuyo objetivo era conseguir una moneda descentralizada y sustituir la ya existente para dar un medio de intercambio *peer-to-peer* (Tabla 2; Buzzi *et al*., 2018; Mane *et al*., 2022).

Tabla 2. Comparación de divisas tradicionales con las criptomonedas (Buzzi *et al*., 2018).

Divisas tradicionales	Criptomonedas
Físicas	Digitales
Vinculadas a un país concreto	Globales
Emitidas por gobiernos	Ofrecidas a través de minería
La oferta la controlan los bancos centrales	La oferta la controlan los mineros y la tecnología de minería
Se introducen en el sistema económico a través de bonos y otros títulos	Se introducen directamente en el mercado de criptomonedas
Reciben gran influencia de las tasas de inflación y de interés	Reciben poca influencia de política monetaria

Una criptomoneda se puede definir como un activo virtual utilizado como una forma de moneda digital que se intercambia para transferir activos y otras formas de instrumentos financieros y que no está controlada por un órgano de gobierno, como un sistema bancario u otra institución financiera (Delfabro *et al*., 2021). En su lugar, utiliza un libro mayor, que emplea métodos contables para registrar cada operación a través de la tecnología *blockchain* (Rice, 2019).

En la actualidad existen muchas criptodivisas y, es por ello, por lo que, en ocasiones, pueden ser difíciles de diferenciar. No existe una única clasificación aceptada de los diversos tipos de criptomoneda. En este caso, el criterio utilizado fue según su propósito. Cabe señalar que, a pesar de que existen diferencias sutiles entre una moneda virtual, una moneda digital y un *token*, se suelen emplear indistintamente (Rose, 2015).

- **Moneda virtual**. En 2012, el Banco Central Europeo, definió la moneda virtual como “un tipo de dinero digital no regulado, emitido y generalmente controlado por sus creadores, y utilizado y aceptado entre los miembros de una comunidad específica”. Afirma que, aunque una moneda virtual funciona como una moneda tradicional, no tiene los mismos atributos.

- **Moneda digital**. Es una forma de moneda virtual que se crea y almacena electrónicamente. Dentro de este grupo se encuentran las criptomonedas, las monedas estables y las monedas digitales de los bancos centrales (*Central Bank Digital Currency*, CBDC). Es importante hacer una especial mención a esta última, ya que, debido a la digitalización de la sociedad, los bancos centrales han empezado a considerar la posibilidad de emitir dinero digital, como es el caso de la moneda *E-krona* en Suecia. La principal característica de una CBDC como la *E-krona* es que es la primera moneda digital emitida y respaldada por una autoridad monetaria reconocida (*Riksbank*) que garantiza su solvencia como medio de pago, lo que la diferencia de las dos monedas anteriores (Sveriges Riksbank, 2017; Armelius *et al*., 2018).

- ***Tokens***. Son unidades de valor que las organizaciones o proyectos basados en *blockchain* desarrollan sobre las redes de *blockchain* ya existentes. A pesar de

que a menudo comparten una gran semejanza con las criptomonedas de esa red, son una clase de activos digitales completamente diferentes. Son más sencillos de crear, con diversas utilizadas y suelen ser fungibles, es decir, se consumen con el uso.

3.1. MINADO DE CRIPTOMONEDAS

La minería es el proceso integral donde se realiza la generación, transmisión y validación de transacciones de las criptomonedas. Garantiza una propagación estable, y segura de la moneda del pagador al beneficiario. Los bancos que generan la moneda física y monitorizan las transacciones requieren una gran infraestructura para funcionar y operar (Berentsen and Schär, 2018; Krishnan *et al*., 2015). Las criptomonedas superan esta necesidad al implementar un sistema de minería donde las personas en la red, llamadas mineros, son los que monitorizan y validan las transacciones (esto es, la transferencia de monedas de una billetera a otra). Las transacciones realizadas durante un período de tiempo determinado se recopilan para formar un bloque y finalmente se registran y mantienen en la *blockchain*. Cada transacción contiene el *hash* de la transacción anterior realizada por el propietario a través del cual se prueba la autenticidad de una transacción actual, validándola (Berentsen and Schär, 2018). Los mineros también inhiben el gasto doble de la moneda a través de este proceso de validación. Por lo tanto, el objetivo principal de la minería es generar y liberar monedas (Krishnan *et al*., 2015).

La minería de criptomonedas se realiza a través de máquinas diseñadas específicamente para tal propósito, que son las denominadas máquinas de minería (Krishnan *et al*., 2015). El crecimiento periódico de la dificultad de la minería condujo a la evolución de nuevas máquinas con mayor eficiencia que las máquinas diseñadas anteriormente. El coste y el rendimiento de la máquina minera determina su rentabilidad, por lo tanto, su diseño e implementación son muy importantes en la minería. Las diversas máquinas utilizadas en la minería son (Krishnan *et al*., 2015):

- **UPC (*Central Processing Unit*)**. Durante el inicio de la minería, la CPU se utilizó para extraer las monedas de manera efectiva con tasas de *hash* inferiores o iguales a 10 *Mega Hashes* por segundo (MH/seg). No obstante, debido al constante aumento de la dificultad en la minería, el uso de la CPU se volvió irrelevante para las máquinas en evolución con tasas de *hash* más altas. Un *software* de minería popular para la minería de CPU fue *cpuminer*. Este es un programa simple que realiza minería agrupada o minería en solitario.

- **GPU (*Graphics Processing Unit*)**. El poder de la minería de CPU no satisfizo las crecientes demandas, por lo que se emplearon las CPU con tarjetas gráficas para extraer las monedas. Estas tarjetas contienen GPU, que se utilizan para resolver funciones de cálculo matemático complejo. No obstante, esta minería se encuentra en un estado de inactivación, ya que su dificultad ha superado los niveles en los que puede competir, además de tener un alto coste y bajo rendimiento, haciéndola poco competente.

- **FPGA (*Field Programmable Gate Array*)**. Con el fin de solventar los problemas acarreados de la minería GPU, aparece la FPGA que contiene bloques lógicos programables (*Configurable Logic Blocks*, CLB) individuales, los cuales están interconectados de manera que se pueden reconfigurar de manera flexible. Además, son más fáciles de sintetizar, considerándose una buena opción para

la minería de *Bitcoin*. Por otro lado, son reutilizables, ya que se pueden reprogramar fácilmente y consumen una quinta parte menos de energía que la GPU.

- **ASIC (*Application Specific Integrated Circuit*)**. Ofrecen un rendimiento mejorado de los FPGA en la minería a gran escala, ya que están diseñados específicamente para calcular *hashes* lo más rápido posible, consumiendo la menor cantidad de energía. Los ASIC de *Bitcoin* son buenos para las tareas matemáticas complejas que necesita la minería, extrayendo *Bitcoins* de la manera más rápida y eficiente posible. Debido a sus ventajas en comparación con las otras máquinas de minería disponibles, los ASIC actualmente están reinando en el campo de la minería con su rendimiento.

3.2. FUNCIONES DE LAS CRIPTOMONEDAS

Es importante diferenciar las posibles funciones de las criptomonedas, ya que estas, al igual que el dinero convencional, pueden ser destinadas a diferentes utilidades por sus poseedores (Buzzi *et al.,* 2018).

- **Depósito de valor**. Al igual que en el caso de las monedas tradicionales, las criptomonedas tienen como función principal conservar el valor o poder adquisitivo durante un largo periodo de tiempo en las billeteras digitales para poder ser recuperado o intercambiado en el futuro (Aziz, 2019). Dentro de este apartado se pueden incluir tanto las criptomonedas como los *tokens*, siendo el más significativo el *Bitcoin*. En su caso, el número de monedas que se puede minar es limitado, por lo que es más factible que mantenga el valor a lo largo del tiempo.
- **Medio de intercambio**. Engloban aquellas criptomonedas y *tokens* que pueden ser utilizadas para la adquisición de bienes y servicios, al igual que las monedas *fiat* (monedas de curso legal emitidas por un banco central del gobierno de un país como puede ser el euro). Para que puedan cumplir con esta función, el comerciante debe aceptarlas como medio de pago, algo que no es muy común, aunque puede llegar a serlo en el futuro (Aziz, 2019). Las más utilizadas en este sentido son: *Bitcoin*, *Ether* o *Dogecoin* (ver apartado 3.3).
- ***Tokens* de intercambio**. Se utilizan dentro de plataformas en las que se suelen ofrecer como recompensa a los usuarios de manera que incentiven así la actividad. A menudo este tipo de *tokens* solo tiene utilidad dentro de la red en la que han sido creados.

Es importante mencionar que para que las criptomonedas sean consideradas como dinero, tienen que cumplir cuatro funciones (Buzzi et al., 2018):

- Medio de cambio: el dinero como medio de cambio consigue eliminar la necesidad de la doble coincidencia de deseos, requisito indispensable en la clásica economía de trueque.
- Depósito de valor: se trata de un activo que mantiene su valor en un largo periodo de tiempo.
- Unidad de cuenta: es la unidad para medir los precios y llevar todo tipo de cuentas.
- Patrón de pagos diferidos: son utilizadas en las transacciones cuya duración se extiende en el largo plazo.

Las dos últimas funciones, aunque habituales, no son necesarias. Las criptomonedas podrían no ser consideradas dinero al no ser aceptadas como medio de pago en cualquier transacción. En cuanto al requisito del depósito de valor tampoco lo cumplirían, debido a la gran volatilidad que han mostrado a lo largo del tiempo la mayoría de ellas, no podrían ser consideradas depósito de valor ni siquiera en el corto plazo. Por ello, podríamos concluir que las criptomonedas se asemejan más a las materias primas, puesto que:

- El valor de la criptomoneda no se vincula de manera exclusiva al comportamiento de una sola economía.
- Los cambios en el tipo de interés y en la cantidad de reservas monetarias tienen un efecto indirecto en su valor.
- Su valor va a depender de que los usuarios mantengan el precio de conversión a monedas tradicionales.

3.3. TIPOS DE CRIPTOMONEDAS

Desde la aparición del *Bitcoin* en 2008 han ido apareciendo gran cantidad de criptomonedas basadas en la tecnología de la cadena de bloques. No obstante, el *Bitcoin* continúa siendo el de mayor capitalización de mercado (Figura 2).

Figura 2. Porcentaje de la capitalización de mercado total (https://coinmarketcap.com/es).En este gráfico se pueden observar las proporciones de los 10 criptoactivos de mayor importancia en la actualidad dentro de la capitalización total de todos los activos.

Bitcoin. Es la criptomoneda de mayor capitalización de mercado. Actualmente es aceptada como moneda de curso legal en El Salvador y la República Centroafricana (El Confidencial, 2022). Es un sistema de pago entre sus usuarios (Figura 3), que pueden utilizarlo a través de una aplicación de su móvil u ordenador, desde la que acceden a su *wallet* personal con el que pueden realizar operaciones sin intermediarios con la utilización de claves pública y privada. Toda operación realizada con *Bitcoin* queda

registrada de manera permanente en la cadena de bloques. El protocolo de esta criptomoneda es de código abierto, por lo que su código de programación es de libre disposición, pudiendo los usuarios redistribuirlo. Cualquier usuario con un ordenador lo suficientemente potente podría procesar un bloque de la cadena y obtener así una recompensa en *Bitcoins*. El algoritmo del *Bitcoin* fue creado para que en el año 2.140 se extraigan todos los *Bitcoins,* con un límite total de 21 millones, de ahí su denominación como minería (Caurín, 2017). Por ello las recompensas por minar un bloque disminuyen con el paso del tiempo, reduciéndose a la mitad cada 4 años, siendo inicialmente la recompensa de 50 *Bitcoins* (Ordinas, 2017).

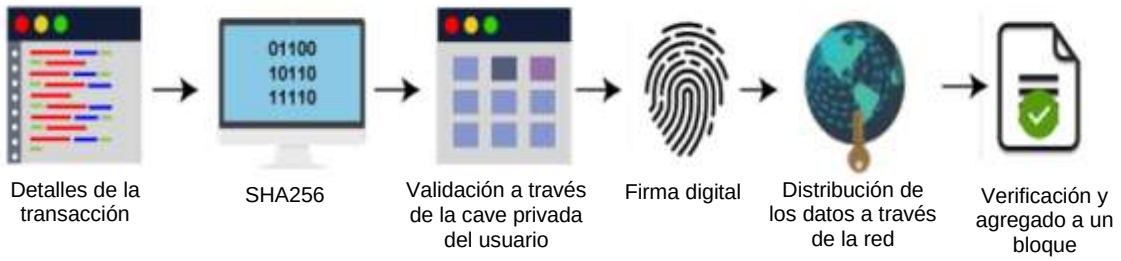


Figura 3. Transacción *Bitcoin*. SHA, *Secure Hashing Algorithm*; SHA256, algoritmo de minería del protocolo *Bitcoin* referente a la función *hash* criptográfica que genera un valor de 256 *bits* de longitud (Mane *et al*., 2020).

Ethereum. Es la segunda plataforma de *blockchain* a nivel de capitalización de mercado. Fue creada por Vitalik Buterin, co-fundador de *Bitcoin* Magazine que comenzó a desarrollar *Ethereum* en 2014 (Miranda, 2018). La criptomoneda propia es el *Ether*. Sus propiedades son similares a las del *Bitcoin* en cuanto a la realización de pagos, siendo el incentivo utilizado para los mineros que incluyen bloques en la cadena. Actualmente utiliza el mecanismo de PoW, pero está previsto que en 2023 pase a utilizar el PoS en su denominada *blockchain Ethereum* 2.0 (Callejo, 2021). Este cambio ha sido provocado por la alta demanda que ha llevado al límite de sus capacidades a la *blockchain* por la irrupción de las DeFi, las DApps y los *tokens* no fungibles (ver apartado 4). Con este cambio, aparte de eliminar el enorme consumo eléctrico provocado en la minería, se aumenta la capacidad de procesamiento de las transacciones. Su funcionamiento se puede ver en la siguiente imagen (Figura 4).

Figura 4. Representación esquemática del funcionamiento de *Ethereum* (https://www.ig.com/es-/ethereum-trading/que-es-ether-y-como-funciona).

***Binance Coin*.** Es la criptomoneda creada por *Binance* para actuar como motor de su red *Binance Chain*. Se trata de un *token* dentro de la red *Ethereum* lanzado en el 2017, iniciando con una venta de 200 millones de estas monedas. De manera posterior a la creación de la criptomoneda, la plataforma creó la red propia *Binance Chain* (Ferry,

2022). Esta criptomoneda no se puede minar, si no que utiliza un tipo de consenso donde tan solo pueden participar una serie concreta de validadores que consiguen la moneda al verificar los bloques. El límite está establecido en 200 millones de *tokens*. (Otero *et al.,* 2022). Algunas de sus funciones más relevantes son (Romo, 2021):

- Al realizar pagos dentro de la red se obtiene un descuento en las comisiones aplicadas.
- Es fácilmente intercambiable por otras criptomonedas como *Bitcoin* o *Ether*.
- Puede utilizarse como medio de pago.
- Es el *token* principal de la *Binance Smart Chain*, que es una plataforma de contratos inteligentes.
- Al poseer esta criptomoneda se puede participar en sorteos ofrecidos dentro de la plataforma.

***DogeCoin*.** Creada en 2013 por Billy Markus y Jackson Palmer Markus (Medina *et al.*, 2016). Esta criptomoneda utiliza un perro como símbolo basado en un conocido meme de internet llamado *Doge* (Medina *et al.*, 2016). Esta moneda está basada en el protocolo *Bitcoin* con algunas modificaciones (Medina *et al.*, 2016). En el momento de su creación, el *Bitcoin* estaba siendo muy criticado ya que se le relacionaba con muchas transacciones de la denominada *Dark Web*, esto es operaciones ilegales. Es por esto por lo que sus creadores idearon una criptomoneda que no tuviera ninguna relación con este tipo de asuntos. Su funcionamiento es similar al de otras criptomonedas, utilizando el mecanismo del PoW para el minado de sus *tokens*, siendo este notablemente más veloz que el de *Bitcoin*, al igual que los pagos realizados con esta criptomoneda, que también son más rápidos (Medina *et al.*, 2016). Según su algoritmo, el máximo de *Dogecoins* que pueden ser minadas es de cien mil millones de unidades (Medina *et al.*, 2016).

3.3.1. *STABLECOINS*

A parte de estas importantes criptomonedas cabe destacar a las criptomonedas estables (*stablecoins).* Estas tratan de disminuir la volatilidad del resto de monedas virtuales. Se trata de monedas digitales construidas de tal manera que su volatilidad está limitada por diseño. Pueden estar ligados al valor de una moneda *fiat*, a bienes materiales como el oro e incluso a otra criptomoneda (González-Páramo, 2019). Existen diversos tipos de monedas estables, que se pueden clasificar en dos grandes grupos:

- **Colaterizadas**: su mecanismo de estabilización se basa en el principio de dinero fiduciario. Su valor está referenciado a un colateral (BBVA, 2019). Dentro de este grupo existen a su vez tres categorías diferentes:
    - Respaldadas con monedas *fiat*: destacan las *stablecoins Tether* y *TrueCoin*, las dos se encuentran bajo el respaldo del dólar estadounidense. El *Tether* fue creado en el año 2014 utilizando la tecnología de la *blockchain* y actualmente su capitalización de mercado ronda los 68.000 millones de dólares (Neocripto, 2022). Sus clientes deben depositar dólares en la plataforma por los que recibirán *tokens*, en este caso denominados *USDT* (Martínez, 2020), que pueden usarse como cualquier criptomoneda. La ventaja es que, según la compañía,

existe una reserva de dólares suficiente para garantizar el depósito de los clientes. Es decir, los usuarios podrían volver a cambiar sus *USDT* por dólares cuando quisiesen sin verse afectados por las fluctuaciones típicas de las criptomonedas. Sin embargo, existen dudas de que realmente la compañía cuente con la cantidad de dólares necesaria para cubrir toda la inversión (Martínez, 2020).

- Respaldadas con otra criptomoneda: dentro de este grupo se encuentra *DAI* (BBVA, 2019). Esta criptomoneda utiliza como respaldo a su valor la plataforma *Ethereum* y el valor del *Ether*. Los usuarios deben depositar *Ethers* a cambio de *DAI*, pero utilizando el mecanismo de sobrecolaterización, es decir, dejando un exceso de depósito y obteniendo por contrapartida una reducción del riesgo, previniendo así las pérdidas posibles como resultado de una disminución del valor de esta criptomoneda (BBVA, 2019).
- Respaldadas con otros bienes: en este caso la criptomoneda mantiene su valor fijado al precio de un bien como puede ser el oro. Esta es la situación de *G-Coin*. En esta plataforma cada *token* equivale a un gramo de oro físico. En esta compañía aseguran tener el oro almacenado y que sus *tokens* pueden ser utilizados por los usuarios ya sea para intercambiarlos por oro físico, como depósito de valor o como otras criptomonedas para realizar pagos digitales (BBVA, 2019).

- **No colaterizadas:** se trata de criptomonedas estables controladas por algoritmos, es decir, que no están respaldadas por otro valor externo, solamente por algoritmos con el fin de evitar las variaciones de precio, emitiendo más moneda digital cuando el precio sube y viceversa cuando el precio baja. Estos algoritmos pueden ser mejores o peores y, a veces, no evitan las grandes fluctuaciones en los precios. Como ejemplo está *USDX*, que mantiene el precio ligado al del dólar mediante algoritmos, con el fin de mantenerlo estable. Su sistema opera mediante s*mart contracts* que regulan su funcionamiento.

Debido a su importancia en la actualidad, cabe destacar las siguientes *stablecoins*:

***Binance USD*.** Es una moneda estable cuyo respaldo es el dólar estadounidense. Su emisor es el principal bróker de criptomonedas *Binance* de manera conjunta con Paxos (empresa financiera de infraestructura *blockchain*). Su precio se mantiene siempre constante en un dólar y se encuentra regulada por el Departamento de Servicios Financieros del Estado de Nueva York (NYDFS; Larriva, 2021). Al igual que otras monedas estables fue creada para facilitar las transacciones en las DeFi, consiguiendo ser la primera en recibir la aprobación regulatoria del NYDFS y encontrándose disponible para su compra desde septiembre de 2019 (Criptomonedasweb, 2022). Este *token* emplea varios *smart contracts* para funcionar, facilitando así su interoperabilidad en cualquier intercambio admitido por *Ethereum*. Actualmente continúa siendo uno de los pocos *tokens* regulados que existen en el mercado. Esto unido a su asociación con *Paxos*, le da una gran credibilidad y cierta ventaja en comparación a otras monedas estables de características similares (Criptomonedasweb, 2022).

***USD Coin*.** Su valor está ligado al del dólar estadounidense con una equivalencia 1:1. Al mantener su valor ligado a esta moneda este no varía y tampoco permite ser minado ya que su emisión depende de la empresa que la lanzó (Caligiuri, 2022). Este

proyecto vio la luz en 2018 en colaboración entre *Coinbase* y *Circle Internet Financial*, estando todas sus criptomonedas respaldadas por dólares mantenidos en reserva combinando efectivo y bonos del Tesoro de Estados Unidos a corto plazo (Otero *et al.,* 2022). Esta criptomoneda surge con el objetivo de competir con la criptomoneda *USD Tether* para funcionar dentro del sistema de pagos de sus empresas creadoras. Esta decisión se debe a los problemas de funcionamiento de *Tether*, ya que era una moneda lenta, costosa y que no estaba concebida para el futuro de las redes descentralizadas, funcionando solo en *OmniLayer* y *Bitcoin* (Dolader y Muñoz, 2017). Cabe señalar que este *token* está creado en la red de *Ethereum*, sin verse afectado por las variaciones en el valor del *Ether* (Caligiuri, 2022). Sus principales funciones son *tokenizar* el dólar estadounidense, es decir, cambiar dólares por *tokens*, emplearla para retirar efectivo, realizar transferencias entre direcciones de *Ethereum* y depósitos desde una billetera *Ethereum* externa (Caligiuri, 2022).

3.4. CRIPTOMONEDAS DESAPARECIDAS Y CRIPTOMONEDAS MUERTAS

En los últimos años el número de criptomonedas que han desaparecido ha aumentado de manera continuada. Aunque algunos proyectos consiguen asentarse, otros muchos no lo hacen del mismo modo y terminan por desaparecer al no completar sus objetivos. En este ámbito, debemos diferenciar dos tipos de criptomonedas: criptomonedas desaparecidas (aquellas que no se encuentran en el mercado) y criptomonedas muertas (pueden estar en el mercado, pero a los denominados precios basura). De ahí que estas últimas sean conocidas como *trashcoin* (Martín, 2022).

Actualmente el número de criptomonedas que han desaparecido se estima en un número cercano al millar (Martín, 2022). Los motivos por los que desaparecen o mueren estas criptomonedas no siempre es el mismo, por lo que las agruparemos en diferentes categorías:

- Proyectos fracasados: es el grupo más numeroso dentro de esta clasificación. Existe gran cantidad de proyectos de criptomonedas tanto fracasados como abandonados, también hay que tener en cuenta que en este epígrafe se incluyen los *tokens* digitales, que se trata de un proyecto más sencillo de abordar y ha dado como resultado un gran número de proyectos finalmente abandonados. Por ejemplo, *GetGems* y *NanoHealthCare Token* (Martín, 2022).
- Fraudes: se trata del segundo mayor grupo en cuanto a importancia y con una importancia en aumento. En este se incluyen los proyectos que no son reales, no son legítimos o que son fraudulentos en los que se crea una criptomoneda con el único propósito de aprovecharse del usuario. La desaparición de este tipo de criptomonedas se produce de manera intencionada. Un ejemplo es *OneCoin*. Dentro de este grupo, es importante hacer mención a dos tipos de estafas con criptomonedas:
    - Estafas piramidales: plataformas dedicadas a la inversión que utilizan como reclamo las criptomonedas (Martín, 2022).
    - Estafas *ponzi* con activos digitales: siguen el mismo modelo de estafa, pero de una manera más sofisticada, utilizando un activo digital de creación propia que hace parecer más real el proyecto, siendo de este tipo la ya mencionada *OneCoin*, considerándose que en este caso se llegaron a estafar miles de millones de dólares (Martín, 2022).

- Memes: es el grupo menos común, tratándose de criptomonedas creadas como una especia de broma y que, tras cumplir su función, desaparecen. Un ejemplo es *BoringCoin* (Martín, 2022).

3.5. VENTAJAS Y DESVENTAJAS DE LA UTILIZACIÓN DE LAS CRIPTOMONEDAS

Existen opiniones diversas y enfrentadas sobre el futuro de las criptomonedas. Las visiones optimistas sobre el uso de las criptomonedas se respaldan en el hecho de que facilitan la transferencia de fondos entre las dos partes de una transacción (Bunjaku *et al*., 2017). Estas transferencias se realizan con tarifas de procesamiento mínimas, evitando así los altos costes que cobran la mayoría de los bancos. Así mismo, aquellos países que tienen como objetivo deshacerse del dinero en efectivo tienen un enfoque muy optimista con las criptomonedas (Bunjaku *et al*., 2017). Por otro lado, muchos inversores y economistas muestran un alto escepticismo en el uso de las criptomonedas en el sistema de pagos y transacciones financieras, alegando que se trata de sistemas muy volátiles que pueden usarse para lavar dinero o financiar actividades ilegales (Rice, 2019).

Ventajas de las criptomonedas

- **Privacidad**. Hay una falta de autoridad y regulación sobre las criptomonedas, que permite que el propietario no necesite justificar las compras ante la autoridad, creando una libertad personal de compra (Rice, 2019).
- **Descentralizado**. No existe una autoridad de control central en la red, es decir, no tiene poder para dictar las reglas e incluso si alguna parte de la red se desconecta, el sistema de pago seguirá funcionando de forma estable (Bunjaku *et al*., 2017; Rice, 2019).
- **Sin inflación**. El número máximo de monedas está estrictamente limitado a 21 millones de *Bitcoin*. Como no existen fuerzas políticas ni corporaciones capaces de cambiar esta orden, no hay posibilidad de desarrollar la inflación en el sistema (Bunjaku *et al*., 2017).
- **Red de criptomonedas punto a punto**. No hay un servidor maestro que sea responsable de todas las operaciones. El intercambio de la información, en este caso, de dinero, es entre 2-3 o más clientes de software. Cada cliente almacena un registro de todas las transacciones comprometidas y la cantidad de criptomonedas en cada billetera. Las transacciones son realizadas por cientos de servidores distribuidos. Ni los bancos, ni los impuestos, ni los gobiernos pueden controlar el intercambio de dinero (Bunjaku *et al*., 2017).
- **Posibilidades ilimitadas de transacción**. Cada uno de los titulares de la billetera puede pagar a cualquier persona, en cualquier lugar y en cualquier momento. La transacción no se puede controlar ni prevenir, por lo que puede realizar transferencias a cualquier parte del mundo donde se encuentre otro usuario con una billetera de criptomoneda (Bunjaku *et al*., 2017).
- **Sin límites**. Los pagos realizados en este sistema son imposibles de cancelar. Las monedas no se pueden falsificar, copiar ni gastar dos veces. Estas capacidades garantizan la integridad de todo el sistema (Bunjaku *et al*., 2017; Rice, 2019).
- **Bajo coste de operación**. No es necesario pagar comisiones ni tarifas a los bancos y otras organizaciones. La tarifa de comisión en este sistema es más

baja que en cualquier otro, equivale al 0,1% del importe de la transacción (Bunjaku *et al*., 2017).

- **Fácil de usar**. La empresa necesita aproximadamente 5 minutos para crear una billetera e inmediatamente comienza a usarla sin preguntas ni comisiones (Rice, 2019).
- **Anonimato**. Es completamente anónimo y al mismo tiempo totalmente transparente. Cualquier empresa puede crear un número infinito de direcciones de criptomonedas sin referencia al nombre, dirección o cualquier otra información (Bunjaku *et al*., 2017; Rice, 2019).
- **Transparencia**. Almacenan el historial de transacciones que alguna vez han tenido lugar. Esto es lo que se conoce como *blockchain*. Por lo tanto, si la empresa ha utilizado públicamente la dirección de la criptomoneda, cualquiera puede ver cuánta cantidad posee. Mientras que, si la dirección de la empresa no se confirma públicamente, nadie sabrá nunca que pertenece a esa empresa (Bunjaku *et al*., 2017; Rice, 2019).
- **Velocidad de transacción**. La capacidad de enviar dinero a cualquier lugar y a cualquier persona en cuestión de minutos después de que la red procese el pago (Bunjaku *et al*., 2017; Rice, 2019).
- **Pertenece solo al propietario de la billetera**. Existe un sistema de pago electrónico único en el que la cuenta pertenece exclusivamente al propietario. Por ejemplo, en PayPal, si por algún motivo la empresa decide que el propietario utiliza la cuenta de forma incorrecta, el sistema tiene derecho a congelar todos los fondos de la cuenta sin siquiera advertir al propietario al respecto. La verificación del uso adecuado de la cuenta es responsabilidad total del propietario. Con las criptomonedas, el propietario tiene una clave privada y una clave pública correspondiente, que es la dirección de la billetera (Bunjaku *et al*., 2017). Nadie más que el propietario puede retirar las criptomonedas.
- **Código abierto para minar criptomonedas**. Se aplican los mismos logaritmos que utiliza la banca en línea. La única diferencia de la banca por internet es la divulgación de información sobre los usuarios (Bunjaku *et al*., 2017). Se comparte toda la información sobre la transacción en la red (cómo, cuándo), pero no hay datos sobre el destinatario o el remitente de las monedas (no hay acceso a la información personal de la billetera del propietario).
- **No hay posibilidades de utilizar datos personales para el fraude**. Éste es un punto importante. Hoy en día la mayoría de las compras se realizan con tarjetas de crédito. Al completar formularios en sitios web, los clientes deben ingresar los siguientes datos: número de tarjeta, fecha de vencimiento y código. Es difícil encontrar una forma menos segura de realizar el pago. Por lo tanto, las tarjetas de crédito son a menudo robadas. Las transacciones de criptomonedas no requieren la divulgación de ningún dato personal. En su lugar, utiliza dos claves: pública y privada (Bunjaku *et al*., 2017). La clave pública está disponible para todos (es decir, la dirección de la billetera), pero la clave privada solo la conoce el propietario. La transacción debe firmarse mediante la interacción de claves privadas y la aplicación de una función matemática. Esto crea evidencia de que la transacción es realizada por el propietario.

- **Diversidad que la criptomoneda agrega a la billetera de un inversor**. Independientemente de si el inversor es un administrador de activos, de fondos de cobertura o una persona que trabaja en la jubilación personal, la diversidad es fundamental para el éxito de la billetera a largo plazo (Rice, 2019).

Desventajas de las criptomonedas

- **Falta de familiaridad con las criptomonedas**. Es un gran inconveniente tanto para los inversores como para los usuarios (Rice, 2019).
- **Volatilidad**. Casi todos los altibajos del valor de las criptomonedas dependen directamente de las declaraciones de los gobiernos de los diferentes países. Esta volatilidad crea un problema a corto plazo (Bunjaku *et al*., 2017; Rice, 2019).
- **Desconfianza en el producto y el sistema**. La criptomoneda se sustenta de la confianza y aceptación de sus propietarios y usuarios. Las instituciones financieras típicas están respaldadas por el gobierno federal, por lo que el riesgo para el inversionista es mínimo cuando se trata de un fallo repentino. La criptmoneda no tiene seguro y no puede garantizarse contra pasivos ni pagarse con otros activos, como pueden hacerlo los bancos u otras instituciones (Bunjaku *et al*., 2017; Rice, 2019).
- **Falta de aceptación**. Debido a su relativa novedad, hay pocos cajeros automáticos criptográficos y muchas instituciones financieras no reconocen las criptomonedas como moneda rea. Junto con esta falta de aceptación, viene la falta de capacidad para comprar artículos regulares (combustibles, comida o ropa; Rice, 2019).
- **Uso de criptomonedas con fines ilegales y delictivos**. Su uso por parte de estafadores y piratas informáticos es un peligro. También pueden ser utilizadas por el crimen organizado para el lavado del dinero, para financiar grupos terroristas o para otras actividades ilegales que pueden ocultarse debido al anonimato de las criptomonedas (Bunjaku *et al*., 2017; Rice, 2019).
- **Incertidumbre**. El futuro es impredecible, no se sabe si la criptomoneda es solo una moda pasajera y solo existirá durante unos años más, lo que genera un inconveniente para los principales inversores (Rice, 2019).

3.6. EVOLUCIÓN DE LAS CRIPTOMONEDAS

Una de las características fundamentales de las criptomonedas es su gran volatilidad a lo largo del tiempo, combinando etapas de auge con los “criptoinviernos”, entendidos como periodos duraderos de disminución de su valor (Muñon-Ledo, 2022).

En 2017, el *Bitcoin*, utilizada como valor de referencia de este mercado, alcanzó una gran cotización, llegando a los 17.000 dólares. Sin embargo, un año más tarde, se produjo una bajada de su valor (debido a la falta de una forma de regulación común en los diferentes países), alcanzando los 3.400 dólares (Muñon-Ledo, 2022). Posteriormente, con la llegada de la pandemia (a mediados del 2019), se produjo un aumento de la demanda y, como consecuencia, una subida de su valor, ya que los usuarios empezaron a ver las criptomonedas como un refugio a la inflación, alcanzando su máximo histórico a finales del 2021, rozando los 70.000 dólares (Paxful, 2022).

El incremento de la inflación y las políticas monetarias contractivas adoptadas por los bancos centrales han provocado una enorme caída en el presente año (Planner Financiero, 2022), situando al *Bitcoin* por debajo de los 20.000 dólares a finales del mes de junio (CoinMarketCap, 2022).

Por lo tanto, podemos concluir que con un futuro aún incierto son muchas las especulaciones respecto al futuro de las criptomonedas, lo que hace muy complicado vaticinar si su valor aumentará o, por el contrario, su caída será aún mayor.

4. *TOKENS* NO FUNGIBLES

Los *tokens* no fungibles (*Non Fungible Token*, NFT) surgen en 2014, en Nueva York, pero no fue hasta 2020 cuando se dieron a conocer a nivel mundial (Zúñiga, 2022), protagonizando noticias por sus ventas millonarias en segmentos como el arte y los objetos digitales coleccionables. El concepto de *tokens* no fungibles se propuso originalmente a partir de un *token* estándar de *Ethereum* y su propósito era diferenciar cada *token* con signos distinguibles (Zúñiga, 2022).

Los NFT se almacenan en una cadena de bloques pública y transparente que se puede usar para representar la propiedad de activos digitales. Es decir, son aplicaciones descentralizadas con altos niveles de verificabilidad, resistencia a la manipulación, usabilidad, atomicidad y trazabilidad (Pinto-Gutiérrez *et al*., 2022).

La principal diferencia entre los NFT y las criptomonedas es que estas últimas son fungibles o intercambiables y todas valen la misma cantidad (es decir, un *Bitcoin* es igual a otro *Bitcoin*; Lau, 2020). Sin embargo, los NFT no son fungibles, lo que significa que no pierden sus propiedades tras el uso. Precisamente esta singularidad permite el uso de los NFT para autenticar la propiedad de los activos digitales (Lau, 2020; Bao and Roubaud, 2022). En consecuencia, podemos establecer las principales características de los NFT como:

- **Único**. Los *tokens* no fungibles contienen dentro de su código información que describe las propiedades de cada *token* que los hacen diferentes a los demás.
- **Rastreable**. Cada NFT tiene un registro de transacciones en cadena, desde que se creó, incluso cada vez que cambió de manos. Esto significa que cada *token* puede ser verificablemente auténtico y no una falsificación.
- **Raro**. Para que los *tokens* no fungibles sean atractivos para los compradores, deben ser escasos. Esto garantiza que los activos sigan siendo deseables a largo plazo y que la oferta no supere la demanda.
- **Indivisible**. Los NFT en su mayoría no se pueden negociar como fracciones de un todo. No se pueden dividir en denominaciones más pequeñas.
- **Programable**. Como todos los activos digitales tradicionales y *tokens* creados en cadenas de bloques de contratos inteligentes, los NFT son totalmente programables.

En otras palabras, las NFT combinan las mejores características de la tecnología *blockchain* descentralizada con activos no fungibles. A diferencia de los activos digitales regulares que son emitidos y regulados por entidades centralizadas, que se le pueden quitar en cualquier momento, es posible poseer y controlar realmente sus propios NFT (Lau, 2020).

Como se ha dicho previamente, los NFT se pueden utilizar para representar una obra de arte, un contrato de futuros, una partitura musical, un libro o cualquier tipo de objeto que pueda considerarse único o raro. De ahí que los investigadores clasifiquen los NFT en seis categorías principales según los escenarios en los que se usan más ampliamente: arte, coleccionables, juegos, metaverso, otros y utilidad (Bao and Roubaud, 2022). Cabe señalar que los NFT se venden en mercados especializados como, *OpenSea*, *Axie Marketplace* y *Rarible* (Bao and Roubaud, 2022).

5. CONCLUSIONES

- La tecnología *blockchain* es un sistema descentralizado, lo que también conlleva problemas como la falta de regulación por parte de los estados, algo que aumenta la incertidumbre para todo aquel ajeno a esta tecnología, ya que aún es vista como algo demasiado volátil y poco arraigado en la sociedad. Además, no está exenta de vulnerabilidades, como pueden ser ataques externos o errores de programación.

- Este sistema está emergiendo como un enfoque comercial para organizaciones en diferentes ámbitos, incluidos productos de consumo, fabricación, servicios financieros, atención médica, ciencias biológicas y sector público. Esto se consigue gracias a que la cadena de bloques aumenta la confianza, la inmutabilidad, la transparencia y la seguridad junto con la reducción de tiempo y costes.

- Además de las cadenas de bloques, los contratos inteligentes se están desarrollando rápidamente, aunque aún quedan varios desafíos por resolver, como el lenguaje de la programación, su seguridad y su privacidad.

- Las finanzas descentralizadas siguen siendo un mercado con ciertos riesgos pero que también ofrecen unas oportunidades interesantes en términos de eficiencia, transparencia e inmutabilidad, que contribuyen a crear una infraestructura financiera más sólida.

- La adopción de la criptomoneda como moneda legal parece la evolución más lógica, aprovechando así su rapidez, eficiencia y seguridad. Su aceptación conllevaría una serie de beneficios como evitar la evasión de impuestos, estafas, el lavado de dinero y su volatilidad, que obstaculizan significativamente su reputación. Por lo que, aprovechar la innovación en lugar de suprimirla, aumentaría sus ventajas y lograría un gran avance especialmente en materia jurídica.

- Los *tokens* no fungibles combinan las mejores características de la cadena de bloques descentralizada con activos no fungibles para crear *tokens* únicos y auténticos. Sin embargo, todavía les queda un largo camino por recorrer antes de alcanzar la adopción masiva, debido a la inaccesibilidad, la dificultad para vincular los activos del mundo real y la falta de regulación.

6. BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS:

Aggarwal, S. y Kumar, N. (2021): "Basics of blockchain", Advances in computers, nº 121, pp, 129-146.

Armelius, H., Boel, P., Claussen, C. A. y Nessén, M. (2018):" The e-krona and the macroeconomy", Penning-OCH valutapolitik, nº 3, pp, 42-64.

Aziz, A. (2019): "Crytocurrency: evolution and legal dimension", IJBEL, nº 4, pp, 31-33.

Bao, H. y Roubaud, D. (2022): "Non-fungible token: a systematic review and research agenda", Journal of risk and financial management, nº 15, pp, 215.

Beckman, M. (2021): "NFTs Digital Artwork. Blockchain technology", Skyhorse publishing.

Berentsen, A. y Schär, F. (2018): "A short introduction to the world of cryptocurrencies", First Quarter, nº 100, pp, 1-16.

Borrega, R. (2021): "Finanzas Descentralizadas". Trabajo Fin de Grado. Grado en Ingeniería Informática, Universitat Politècnica de València.

Bunjaku, F., Gjorgieva-Trajkovshka, O. y Miteva-Kacarski, E. (2017): "Cryptocurrencies-advantages and disadvantages", Journal of Economics, nº 2, pp, 31-39.

Buzzi, A., Cittadini, M. y De Oliveira, M. (2018): "Introducción a las criptomonedas", XXXIX Jornadas Nacionales de Profesores Universitarios de Matemática Financiera. Facultad de Ciencias Económicas, Universidad Nacional de San Luis (Argentina).

Caligiuri, A. J. (2022): "Criptomonedas y cash management". Trabajo Final. Universidad de Ciencias Empresariales y Sociales (Buenos aires).

Cardozo, G. y Perdomo, P. (2020): "Comparación de plataformas para *smart contracts* basadas en *blockchain*". Trabajo de Fin de Grado. Facultad de Ingeniería, Universidad de la República (Uruguay).

Delfabro, P., King, D. L. y Williams J. (2021): "The psychology of cryptocurrency trading: risk and protective factors", Journal of Behavioral Addictions, nº 10, pp, 201-207.

Dolader, C., Bel, J. y Muñoz, J. (2017): "La *blockchain*: fundamentos, aplicaciones y relación con otras tecnologías disruptivas", Economía industrial, nº 405, pp, 33-40.

García, P. (2018): "*Blockchain* aplicado al sector público", Trabajo Fin de Máster. Máster Universitario en Gestión de la Información, Universitat Politècnica de València.

Garvía, L. (2018): "¿Se puede utilizar *blockchain* contra los monopolios?", *Blockchain* Economía.

Gómez, I. (2018): "*Blockchain*. La revolución en la industria". Tesis de Licenciatura. Universitat Politècnica de Catalunya.

González-Páramo, J. (2019): “La digitalización del dinero”. Anales de la Real Academia de Ciencias Morales y Políticas, Ministerio de Justicia, pp, 257-278.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. y Bani-Hani, A. (2021): “Blockchain smart contracts: applications, challenges and future trends”, Peer-to-Peer Networking and Applications, nº 14, pp, 2901-2925.

Krishnan, H., Saketh, S. y Vaibhav, V. T. (2015): “Cryptocurrency mining – transition to cloud”, IJACSA, nº 9, pp, 115-124.

Larriva, I. D. (2021): **“**Criptomonedas, ICOs y Stablecoins, la problemática del uso ilícito”. Trabajo de Fin de Grado. Grado en Finanzas y Contabilidad, Universidad de Sevilla.

Lau, K. (2020): “Non-fungible tokens: a brief introduction and history”, Crypto.com.

Legerén-Molina, A. (2018): “Los contratos inteligentes en España (La disciplina de los *smart contracts*)”, Revista de Derecho civil, nº 5, pp, 193-241.

Manca, A. (2022): “Opere d’arte nell’epoca degli NFT: facciamo il punto”. Artribune.

Mane A., Magar, S., Patil, S., Pandit, S. y Ovale, S. (2022): “Crytocurrency: Evolution in finance”, IRJET, nº 5, pp, 282-284.

Martínez, J. (2020): **“**Valor y futuro de las criptomonedas: Análisis crítico”. Trabajo de Fin de Grado. Grado en Comercio, Universidad de Valladolid.

Medina, M. F. y Herrera, J. (2016): “Análisis y comparación de monedas criptográficas basadas en la tecnología *blockchain*”. Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC), Universidad Autónoma de Barcelona.

Miranda, P. (2018): “Explorando la *Blockchain* de *Ethereum* y el desarrollo de *smart contracts*”. Trabajo Final de Grado. Grado en Ingeniería de Sistemas de Telecomunicaciones, Grado en Ingeniería Telemática. Universitat Politècnica de Catalunya.

Nadler, D., De Araújo, H. X. y Santos, C. (2021): “A literatura review about smart contracts technology”, IJAERS, nº 8.

Nakamoto, S. (2008): “Bitcoin: a peer-to-peer electronic cash system”.

Ordinas, M. (2017): “Las criptomonedas: ¿oportunidad o burbuja?”, Banca March, Informe mensual de estrategia.

Otero, M. y Oliver, P. (2022): “Criptomonedas, *stablecoins* y la cripto-economía: el estado de la cuestión”, Documento de trabajo, 2.

Parrondo, L. (2018): “Tecnología *blockchain*, una nueva era para la empresa”, Revista de Contabilidad y Dirección, nº 27, pp, 11-31.

Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D. y Velasquez, S. (2022): “The NFT hype: what draws attention to nong-fungible tokens”, Mathematics, nº 10, pp 1-13.

Piscini, E., Hyman, G. y Henry, W. (2017): “Blockchain: trust economy”, Tech Trends, Deloitte University Press.

Porxas, N. y Conejero, M. (2018): "Tecnología *blockchain*: funcionamiento, aplicaciones y retos jurídicos relacionados", Actualidad Jurídica, nº 48, pp, 24-36.

Preukschat, A., Kuchkovsky, C., Gómez, G., Díez, D. y Molero, I. (2016): "*Blockchain*: la revolución industrial de internet", Gestión 2000.

Puentes, R. (2019): **"***Blockchain* en la música: un método que protegerá la industria", TIA, nº 7, pp, 22-28.

Rice, M. (2019): "Cryptocurrency: history, advantages, disvantages and the future", Senior Honors hereses, nº 933.

Romo, L. (2021). "Análisis económico de criptoactivos y tecnología *blockchain*". Trabajo de Fin de Grado. Grado en Administración y dirección de Empresas, Universidad de Salamanca.

Rose, C. (2015): "The evolution of digital currencies: bitcoin, a cryptocurrency causing a monetary revolution", IBERJ, nº4, pp, 617-622.

Sakiz, B. y Gencer, A. H. (2021): "Blockchain beyond cryptocurrency: non-fungible tokens", Finance, nº 5, pp, 144-151.

Segura, J. M. (2021): "De las criptomonedas y *blockchain* a DeFi: el caso del mercado *blockchain* de futuros de AOVE". Trabajo Fin de Grado. Facultad de Turismo y Finanzas, Universidad de Sevilla.

Statista (2022): "Market capitalization of transactions globally involving a non-fungible token (NFT) from 2018 to 2020".

Sveriges Riksbank (2017): "The Riksbank's e-krona proyect", Report 1, Sveriges R

Trautman, L. J. y Molesky, M. J. (2018): "A primer for blockchain", UMKC Law Review, nº 88.

Vergel, R. A. (2019): "*Blockchain*: auditoría, contabilidad y normativa". Trabajo de Fin de Máster. Facultad de Ciencias Económicas y Empresariales, Universidad de Almería.

Whitaker, A. (2018): "The eureka momento that made bitcoin possible", Dow Jones.

Zemlianskaia, A. (2017): "Tecnología *blockchain* como palanca de cambio en el sector financiero y bancario". Trabajo de Fin de Máster. Máster universitario en estudios avanzados en Dirección de Empresas, Universidad de Sevilla.

Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J. y Imran, M. (2019): "An overview on smat contracts: challenges, advances and platforms", Future Generation Computer Systems, nº 105, pp, 475-491.

Zozaya, C., Incera, J. y Franzoni, A. L. (2019): "*Blockchain*: un tutorial", Estudios, nº 129, pp, 113-126.

Zúñiga, L. (2022): "¿Qué son y cómo se utilizan actualmente los NFT?", Investiga, TEC, nº 4, pp, 3-6.

PÁGINAS WEB CONSULTADAS:

Alonso, I. (2017): Claves que determinarán el éxito o fracaso de las criptomonedas. El economista: https://www.eleconomista.es/opinion-blogs/noticias/8814684/12/17/Claves-que-determinaran-el-exito-o-fracaso-de-las-criptomonedas.html (Consultada el 6 de junio de 2022).

Callejo, G., (2021): ¿Qué es *Ethereum* 2. 0? Todo lo que necesitas saber sobre los cambios de esta *blockchain*. Observatorio Blockchain: https://observatorioblockchain.com/ethereum/que-es-ethereum-2-0-todo-lo-que-necesitas-saber-sobre-esta-blockchain/ (Consultada el 25 de junio de 2022).

Caurín, J. (2017). Tipos de criptomonedas. https://www.economiasimple.net/tipo-de-criptomonedas.html (Consultada el 02 de julio de 2022).

Civieta, O. F. (2021): 10 criptomonedas muertas como la de "El juego del calamar". Business Insider: https://www.businessinsider.es/10-criptomonedas-muertas-como-juego-calamar-959299 (Consultada el 6 de junio de 2022).

Deloitte, (2022). La revolución del *Blockchain* en la Auditoría Interna. https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/blockchain-auditoria-interna.html (Consultada el 26 de mayo de 2022).

Donohue, B. (2014): ¿Qué es un *hash* y cómo funciona? Kaspersky daily: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/28-06/ (Consultada el 8 de junio de 2022).

Esan Business (2019). Fundamentos de *Blockchain*: ¿qué es un *Merkle tree*?: https://www.esan.edu.pe/conexion-esan/fundamentos-de-blockchain-que-es-un-merkle-tree (Consulta el 12 de junio de 2022).

Fernández, J. (2022). Aplicaciones descentralizadas: ¿Qué son? E. Saurio. https://blog.e-saurio.com/aplicaciones-descentralizadas-que-son/ (Consultada el 02 de julio de 2022).

Fernández, Y. (2022). Qué es el *Dogecoin*, cómo funciona y por qué se ha hecho tan popular. Xakata. https://www.xataka.com/basics/que-dogecoin-como-funciona-que-se-ha-hecho-popular (Consultada el 02 de julio de 2022).

Ferry, R. (2022). BNB, conoce a la criptomoneda *Binance*. Mundiario. https://www.mundiario.com/articulo/economia/bnb-conoce-criptomoneda-binance/20220629124113245414.html (Consultada el 02 de julio de 2022).

Gaspar, I. (2021): Criptomonedas: todo lo que hay que saber sobre este arriesgado activo. El economista: https://marcas.eleconomista.es/deutsche-bank/noticias/11272188/06/210/Criptomonedas-todo-lo-que-hay-que-saber-sobre-este-arriesgado-activo.html (Consultada el 31 de mayo de 2022).

López, R. (2020): Qué es prueba de trabajo, PoW *Proof of Work*. Coinmotion: https://coinmotion.com/es/quees-prueba-de-trabajo-pow-proof-of-work- (Consultada el 8 de junio de 2022).

Martín, I. (2022): Cómo funciona *Binance Pool*: servicio de minería. Finanzas Roams:https://finanzas.roams.es/entidadesfinancieras/binance/binance-pool/ (Consultada el 30 de mayo de 2022).

Muñon-Ledo, R. (2022): El mundo de las criptomonedas se enfría: el auge y caída de las monedas virtuales: https://cnnespanol.cnn.com/2022/06/16/criptomonedas-enfria-auge-caida-moneda-virtual-orix/ (Consultada el 29 de junio de 2022).

Neocripto (2022): Stablecoin Giant Tether (USDT) lucha por mantener el dominio. Criptomonedas Digital: https://criptomonedas.digital/stablecoin-giant-tether-usdt-lucha-por-mantener-el-dominio/ (Consultada el 24 de junio de 2022).

Paxos, T. (2022): Máximos históricos de *Bitcoin*. Paxful: https://paxful.com/university/es/maximo-historico-bitcoin/ (Consultada el 28 de junio de 2022).

Sáez, J. (2022): Las 10 criptodivisas (o criptomonedas) con más futuro. IEBS School: https://www.iebschool.com/blog/criptodivisas-criptomonedas-invertir-finanzas/ (Consultada el 6 de junio de 2022).

Simoes, C. (2022). ¿Qué son los bloques en la tecnología Blockchain? Blog de ITDO: https://www.itdo.com/blog/que-son-los-bloques-en-la-tecnologia-blockchain/ (Consultada el 20 de mayo de 2022).

Woonkly, (2022). ¿Cuántos tipos de *blockchain* existen y cuáles son?: https://academy.woonkly.com/nft/tipos-de-blockchain/ (Consultada el 25 de mayo de 2022).

¿Por qué bajan las criptomonedas en el 2022? (2022). Planner Financiero: https://www.plannerfinanciero.com/articulo/porque-bajan-las-criptomonedas-bitcoin-ethereum (Consultada el 29 de junio de 2022).

¿Qué es *Binance USD* (BUSD) *Stablecoin*? (2022). Criptomonedasweb: https://-criptomonedasweb.com/que-es-binance-usd-busd-stablecoin/ (Consultada el 02 de julio de 2022).

¿Qué es la cadena de bloques (*Blockchain*)? (2015). Bit2Me Academy: https://academy.bit2me.com/que-es-cadena-de-bloques-blockchain/ (Consultada el 20 de mayo de 2022).

¿Qué es un protocolo? (2022). CoinBase: https://www.coinbase.com/es-LA-learn-/crypto-basics/what-is-a-protocol (Consultada el 8 de junio de 2022).

¿Qué es una *Blockchain Wallet*? (2020). ViewNext: https://www.viewnext.com/-que-es-una-blockchain-wallet/ (Consultada el 8 de junio de 2022).

¿Qué son las "*establecoins*" y para qué sirven? (2019). BBVA: https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/ (Consultada el 30 de mayo de 2022).

¿Qué tipo de criptomonedas existen? (2022). Finanzan: https://www.finanzan.-com/2022/04/tipos-criptomonedas.html(C (Consultada el 7 de junio de 2022).

Bitcoin (2022). CoinMarketCap: https://coinmarketcap.com/es/currencies/bitcoin/ (Consultada el 25 de junio de 2022).

Cuadros de criptomoneda mundial: capitalización total del mercado de criptomonedas (2022). CoinMarketCap: https://coinmarketcap.com/es-/charts/ (Consultada el 22 de junio de 2022).

La República Centroafricana se une a El Salvador y adopta el *Bitcoin* como moneda de curso legal (2022). El Confidencial: https://www.elconfidencial.com/mercados/2022-04-27/la-republica-centroafricana-se-une-a-el-salvador-y-adopta-el-bitcoin-como-moneda-legal_3415477/ (Consultada el 28 de junio de 2022).