UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas /UPV

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas

Nuevas fórmulas de financiación mediante la tecnología blockchain

Trabajo Fin de Grado

Grado en Administración y Dirección de Empresas

AUTOR/A: Martinez Calatayud, Pablo

Tutor/a: Miranda Ribera, Eduardo

CURSO ACADÉMICO: 2024/2025

RESUMEN

Este Trabajo de Fin de Grado analiza las nuevas fórmulas de financiación surgidas a raíz de la tecnología *blockchain*, un paradigma que está redefiniendo el acceso al capital para empresas y las oportunidades de inversión. El objetivo principal de la investigación es ofrecer una visión integral de este ecosistema, partiendo de sus fundamentos tecnológicos hasta llegar a sus implicaciones prácticas y regulatorias.

Para ello, se realiza un análisis descriptivo que abarca la arquitectura subyacente de la tecnología *blockchain*, la tipología de *token*s (de utilidad, de seguridad, stablecoins y NFTs) y los innovadores modelos de financiación que habilitan, como las Ofertas Iniciales de Monedas (ICOs), Ofertas de *Token*s de Seguridad (STOs) e intercambios (IEOs e IDOs). Un componente central del estudio es el examen del marco jurídico en desarrollo, con especial énfasis en el Reglamento (UE) 2023/1114 (MiCA), que representa el primer esfuerzo comprensivo a nivel mundial por regular el mercado de criptoactivos, y su transposición en España a través de la CNMV y el Banco de España.

El trabajo se complementa con un análisis de casos de estudio que ilustran tanto el potencial de la tokenización de instrumentos financieros para aumentar la liquidez y la eficiencia, como los riesgos sistémicos y legales evidenciados por colapsos notorios como el de Terra-Luna y litigios como los de Ripple y Binance. Los hallazgos principales revelan una clara evolución desde un mercado no regulado y de alto riesgo hacia un entorno más maduro y supervisado, donde la conformidad regulatoria y la transparencia son clave para la sostenibilidad a largo plazo.

Palabras clave: *Blockchain*, Financiación, Tokenización, Regulación, Criptoactivos

ABSTRACT

This Bachelor's Thesis analyses the new financing formulas emerging from *blockchain* technology, a paradigm that is redefining capital access for companies and investment opportunities. The primary objective of this research is to offer a comprehensive overview of this ecosystem, from its technological foundations to its practical and regulatory implications.

To this end, a descriptive analysis is conducted, covering the underlying architecture of *blockchain* technology, the typology of *token*s (utility, security, stablecoins, and NFTs), and the innovative financing models they enable, such as Initial Coin Offerings (ICOs), Security *Token* Offerings (STOs), and exchange offerings (IEOs and IDOs). A central component of the study is the examination of the developing legal framework, with special emphasis on the EU Regulation 2023/1114 (MiCA), which represents the first comprehensive global effort to regulate the crypto-asset market, and its transposition in Spain through the CNMV and the Bank of Spain.

The work is complemented by an analysis of case studies that illustrate both the potential of financial instrument *token*ization to increase liquidity and efficiency, and the systemic and legal risks evidenced by notorious collapses like Terra-Luna and litigation involving Ripple and Binance. The main findings reveal a clear evolution from an unregulated, high-risk market towards a more mature and supervised environment, where regulatory compliance and transparency are key to long-term sustainability.

Key words: *Blockchain*, Financing, *Token*ization, Regulation, Crypto-Assets

RESUM

Aquest Treball de Fi de Grau analitza les noves fórmules de finançament sorgides arran de la tecnologia *blockchain*, un paradigma que està redefinint l'accés al capital per a empreses i les oportunitats d'inversió. L'objectiu principal de la investigació és oferir una visió integral d'aquest ecosistema, partint dels seus fonaments tecnològics fins a arribar a les seves implicacions pràctiques i reguladores.

Per a això, es realitza una anàlisi descriptiva que abasta l'arquitectura subjacent de la tecnologia *blockchain*, la tipologia de tòquens (d'utilitat, de seguretat, stablecoins i NFTs) i els innovadors models de finançament que habiliten, com les Ofertes Inicials de Monedes (ICOs), Ofertes de Tòquens de Seguretat (STOs) i intercanvis (IEOs i IDOs). Un component central de l'estudi és l'examen del marc jurídic en desenvolupament, amb especial èmfasi en el Reglament (UE) 2023/1114 (MiCA), que representa el primer esforç comprensiu a nivell mundial per regular el mercat de criptoactius, i la seva transposició a Espanya a través de la CNMV i el Banc d'Espanya.

El treball es complementa amb una anàlisi de casos d'estudi que il·lustren tant el potencial de la *token*ització d'instruments financers per augmentar la liquiditat i l'eficiència, com els riscos sistèmics i legals evidenciats per col·lapses notoris com el de Terra-Luna i litigis com els de Ripple i Binance. Les troballes principals revelen una clara evolució des d'un mercat no regulat i d'alt risc cap a un entorn més madur i supervisat, on la conformitat reguladora i la transparència són clau per a la sostenibilitat a llarg termini.

Paraules clau: *Blockchain*, Finançament, *Token*ització, Regulació, Criptoactius

Tabla de contenidos

Tabla de figuras

I. Introducción

1. Planteamiento del problema y justificación

Los sistemas de financiación tradicionales, a pesar de su robustez, se caracterizan por ser procesos a menudo lentos, costosos y centralizados. La intermediación de entidades financieras, los extensos requisitos regulatorios y las altas barreras de entrada limitan el acceso al capital para un gran número de startups y pymes, al tiempo que restringen las oportunidades de inversión para el pequeño inversor. En este contexto, la irrupción de la tecnología *blockchain* ha supuesto un cambio de paradigma, proponiendo un modelo financiero alternativo basado en la descentralización, la transparencia y la eficiencia.

La tokenización, es decir, la representación digital de activos en una *blockchain*, ha abierto la puerta a nuevas fórmulas de financiación (ICOs, STOs, etc.) que permiten a los proyectos captar fondos de una base de inversores global de forma directa y ágil. Sin embargo, este ecosistema emergente no está exento de desafíos significativos. La alta volatilidad de los criptoactivos, la complejidad tecnológica, la incertidumbre regulatoria inicial y la proliferación de proyectos fraudulentos han generado un entorno de alto riesgo para los inversores y un desafío para los reguladores.

Por tanto, se hace necesaria una investigación exhaustiva que aborde este fenómeno desde una perspectiva integral, conectando los fundamentos tecnológicos, los modelos de negocio emergentes y, fundamentalmente, el marco legal que busca aportar seguridad y estabilidad al mercado. Este trabajo se justifica en la necesidad de clarificar el panorama actual de la financiación *blockchain*, proporcionando un análisis estructurado que sirva de guía tanto para emprendedores que exploran estas nuevas vías como para inversores que buscan comprender sus riesgos y oportunidades.

2. Objetivos de la investigación

El objetivo general de este trabajo es realizar un análisis comprensivo de las nuevas fórmulas de financiación basadas en la tecnología *blockchain*, examinando sus fundamentos, el marco regulatorio aplicable, su implementación práctica y los retos asociados.

Para alcanzar este objetivo general, se han definido los siguientes objetivos específicos:

1. Explicar los conceptos fundamentales de la tecnología *blockchain*, incluyendo su historia, arquitectura básica y los mecanismos de consenso que garantizan su funcionamiento.

2. Describir los principales modelos de financiación a través de *token*s (ICO, STO, IEO, IDO), así como la tipología y características de los distintos *token*s (utility, security, stablecoins, NFTs).

3. Analizar el marco regulatorio en desarrollo a nivel internacional, con un enfoque particular en el Reglamento MiCA de la Unión Europea y su proceso de adaptación en la normativa española por parte de la CNMV y el Banco de España.

4. Ilustrar la aplicación práctica y los desafíos del sector mediante el estudio de casos relevantes, incluyendo tanto ejemplos de tokenización de instrumentos financieros como proyectos que han enfrentado controversias legales.

5. Extraer conclusiones y buenas prácticas a partir del análisis realizado, que puedan servir de referencia para futuros proyectos en el ámbito de la financiación descentralizada.

3. Metodología y alcance del estudio

La presente investigación se ha desarrollado siguiendo una metodología descriptiva y analítica, basada en una revisión cualitativa de fuentes secundarias. Se ha realizado un estudio exhaustivo de una amplia gama de documentos, incluyendo publicaciones académicas, informes técnicos (*whitepapers*) de proyectos fundacionales como Bitcoin y Ethereum, documentación oficial de organismos reguladores (Reglamento MiCA, circulares de la CNMV), análisis de instituciones financieras internacionales (FSB, BIS) y artículos de prensa económica especializada. El análisis de casos de estudio se utiliza como herramienta para contextualizar y validar los conceptos teóricos y jurídicos expuestos.

El alcance del estudio se centra en las fórmulas de financiación que implican la emisión de *token*s en *blockchain*s públicas, principalmente sobre el ecosistema de Ethereum. El análisis abarca desde la génesis de la tecnología hasta el estado actual del sector en el año 2025, poniendo especial énfasis en la consolidación del marco regulatorio europeo. Si bien se abordan tendencias globales, el análisis normativo se concentra en el contexto de la Unión Europea y España.

4. Asignaturas del grado relacionadas

Las primeras asignaturas relacionada con esto sería tanto Microeconomía como Macroeconomía, ya que permiten tener un primer entendimiento de que es la economía tanto en la parte global como en la que es a menor escala. Estos conocimientos son cruciales para poder entender la economía global sobre la que muchos de los conceptos de este trabajo se basan.

Seguido de Derecho de la Empresa y Derecho del Trabajo, ya que a pesar de no estudiar durante su currículum materia regulatoria económica, sirvió para poder comprender los conceptos básicos y fundamentales del sistema legislativo. Gracias al aprendizaje de esas ideas fundamentales, ha sido más fácil entender los reglamentos aplicados a los criptoactivos.

Por supuesto, las asignaturas como Introducción a las Finanzas y Matemáticas Financieras y ya finalmente, Economía Financiera y Dirección Financiera han sido útiles para poder desarrollar la tesis del trabajo. Conceptos elementales como los tipos de interés, la deuda de una empresa o un gobierno, la idea de acción o qué es el Banco Central son muchos de los que resultan fundamentales para poder abordar el tema central de este TFG.

II. Marco Teórico: Fundamentos de la Tecnología *Blockchain*

1. Historia y evolución de la tecnología *blockchain*

La idea de una cadena de bloques asegurada criptográficamente tiene sus raíces antes de la creación de Bitcoin. En 1991, Stuart Haber y W. Scott Stornetta describieron por primera vez el concepto de una cadena de bloques protegida criptográficamente con el objetivo de crear un sistema donde las marcas de tiempo de los documentos no pudieran ser manipuladas (Kumar, 2020, pág. 38) Este trabajo pionero se basó en la necesidad de asegurar la integridad y la inmutabilidad de los registros digitales a lo largo del tiempo. En 1992, Haber, Stornetta y Dave Bayer mejoraron este diseño mediante la incorporación de árboles de Merkle, una estructura de datos que permitía agrupar eficientemente múltiples certificados de documentos en un solo bloque, optimizando así el proceso de verificación y almacenamiento. (Sherman, Javani, Zhang, & Golaszewski, 2019, pág. 2) La durabilidad de su sistema se evidencia en la publicación semanal de los hashes de los certificados de documentos de su empresa, Surety, en The New York Times desde 1995, lo que demuestra una aplicación temprana y sostenida de los principios de la cadena de bloques para la integridad de datos. (Sherman, Javani, Zhang, & Golaszewski, 2019, pág. 2).

Paralelamente a estos desarrollos, David Chaum propuso un protocolo con similitudes a la *blockchain* en su disertación de 1982 titulada "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". Este trabajo sentó las bases teóricas iniciales para el desarrollo posterior de la tecnología *blockchain*, abordando el problema fundamental de la confianza en sistemas distribuidos. (Sherman, Javani, Zhang, & Golaszewski, 2019) Chaum también fue pionero en el ámbito de la moneda digital, fundando DigiCash en 1989 y lanzando la criptomoneda eCash en 1995. eCash se centró en la privacidad del usuario a través de técnicas criptográficas avanzadas, pero finalmente no logró una adopción generalizada debido a la falta de apoyo bancario y una infraestructura de internet aún en desarrollo. (Sherman, Javani, Zhang, & Golaszewski, 2019, pág. 2)

Otros investigadores también contribuyeron al panorama conceptual que precedió a la *blockchain* moderna. En 1998, el científico informático Nick Szabo trabajó en la idea de

'bit gold', un concepto de moneda digital descentralizada que exploraba la posibilidad de transferir valor digital sin la necesidad de intermediarios tradicionales. (Martinez & Gonzalez, 2024) En el año 2000, Stefan Konst publicó su teoría sobre cadenas protegidas criptográficamente, ofreciendo ideas para su implementación práctica. (IT Faculty, 2018) Estos esfuerzos tempranos, aunque no culminaron en la *blockchain* tal como la conocemos hoy, demuestran una preocupación constante por resolver los problemas de confianza, seguridad y la necesidad de intermediarios en las transacciones y el mantenimiento de registros digitales. (Martinez & Gonzalez, 2024) La convergencia de estas diversas líneas de investigación en criptografía y sistemas distribuidos preparó el terreno para el avance significativo que representó la invención de la *blockchain* por Satoshi Nakamoto.

La publicación del *whitepaper* de Bitcoin, titulado "Bitcoin: A Peer-to-Peer Electronic Cash System", por el individuo bajo el seudónimo de Satoshi Nakamoto el 31 de octubre de 2008, en medio de la crisis financiera global, se considera el punto de inflexión en la historia de la tecnología *blockchain* (Sherman, Javani, Zhang, & Golaszewski, 2019, pág. 2). Este documento seminal propuso un sistema para realizar pagos en línea directamente entre dos partes sin la necesidad de un intermediario financiero de confianza, abordando directamente las deficiencias percibidas en el sistema bancario tradicional de la época (Roopika, 2020, pág. 2).

La innovación clave de Nakamoto radicó en la combinación de principios criptográficos existentes con un novedoso mecanismo de consenso descentralizado (Yaga, Mell, Roby, & Scarfone, 2018, pág. 13). El diseño incorporó un método similar a Hashcash para marcar el tiempo de los bloques sin depender de una autoridad central, y también introdujo un parámetro de dificultad para regular la velocidad a la que se añaden nuevos bloques a la cadena (Nakamoto, 2008). Esta combinación de tecnologías y conceptos computacionales resolvió varios problemas que habían obstaculizado los intentos anteriores de crear una moneda digital descentralizada.

El año 2014 representó un cambio significativo en la percepción de la tecnología *blockchain*, ya que se comenzó a explorar su potencial para aplicaciones más allá de las criptomonedas, dando lugar al concepto de "*Blockchain* 2.0". Un desarrollo fundamental en esta era fue el lanzamiento de la *blockchain* de Ethereum en 2015, que introdujo la innovadora idea de los *smart contracts*: acuerdos autoejecutables escritos en código y almacenados en la *blockchain*. Esta funcionalidad permitió la creación de aplicaciones

descentralizadas (*dApps*) y amplió enormemente la utilidad de la *blockchain* más allá de la simple transferencia de valor digital. (Asmare, Legese, & Birara, 2023, págs. 11-12).

La motivación principal detrás de la creación de Bitcoin por Satoshi Nakamoto fue establecer una versión puramente entre pares de efectivo electrónico que permitiera enviar pagos en línea directamente de una parte a otra sin depender de instituciones financieras como terceros de confianza. Esto surgió de un deseo de superar las debilidades inherentes del modelo basado en la confianza en los sistemas de pago tradicionales, incluyendo la posibilidad de transacciones reversibles, el aumento de los costos de transacción debido a la mediación y el costo más amplio de requerir confianza. (Roopika, 2020, pág. 2)

La evolución posterior de la tecnología *blockchain* ha sido impulsada por el reconocimiento de su potencial para abordar una amplia gama de desafíos en diversos sectores más allá de las finanzas. Las motivaciones incluyen mejorar la transparencia y la rendición de cuentas, mejorar la seguridad y la integridad de los datos, aumentar la eficiencia y reducir los costos y habilitar nuevas formas de aplicaciones descentralizadas y modelos de negocio. El auge de la Industria 4.0 ha amplificado aún más el interés en la *blockchain* para optimizar las cadenas de suministro y garantizar la autenticidad y la trazabilidad de los productos.

2. Conceptos básicos: bloques, nodos, mecanismos de consenso y descentralización

A. Concepto de bloque

Una vez establecida la historia y evolución a lo largo de los años de la tecnología *blockchain,* se va a describir de forma detallada los componentes de la cadena. Esta se fundamenta en una estructura de datos secuencial conocida como cadena de bloques. El bloque es la unidad fundamental que sirve como un contenedor digital de información. Cada bloque dentro de esta cadena actúa como un registro individual que contiene un encabezado y un cuerpo. Para facilitar la compresión, vamos a explicar por separado las dos partes que componen a un bloque: el encabezado y el cuerpo.

El encabezado del bloque alberga metadatos esenciales sobre el bloque en sí, y dentro de él podemos encontrar distintos campos que proporcionan información clave sobre el

bloque, que a continuación se va a detallar de forma breve. Uno de los campos clave es el número de versión, que indica la versión del protocolo que utiliza el bloque, información crucial para las actualizaciones del sistema. Otro campo es la marca de tiempo, que registra el momento en que se creó el bloque, contribuyendo al orden cronológico de la cadena. El siguiente campo es el hash del bloque anterior, que es una huella digital criptográfica del encabezado del bloque que le precede, estableciendo un vínculo seguro entre los bloques y formando la cadena. Este mecanismo de enlace es fundamental para garantizar la integridad e inmutabilidad de la *blockchain*. El campo *nonce* es un valor numérico de 32 bits que se emplea en los sistemas de prueba de trabajo (PoW), que será explicado más adelante. Los mineros manipulan el *nonce* para encontrar un hash que cumpla con el objetivo de dificultad de la red, lo que les permite añadir un nuevo bloque a la cadena. Finalmente, la raíz de Merkle es un hash de todos los hashes de las transacciones dentro del bloque, proporcionando una forma eficiente de verificar la integridad y autenticidad de las transacciones sin necesidad de acceder a la totalidad de los datos del bloque (Wu & Ho, 2023, págs. 2-3). De forma menos técnica, se podría considerar como un resumen digital de todas las transacciones que se incluyen en el cuerpo del bloque.

En contraste con el encabezado, el cuerpo del bloque contiene los datos reales del bloque, que en la mayoría de las *blockchains* consisten en una lista de transacciones. En muchos casos, la primera transacción dentro de un bloque es una transacción especial denominada "*coinbase*", que sirve para recompensar al minero que añadió con éxito el bloque a la cadena (Wu & Ho, 2023, págs. 2-3).

La formación de la cadena de bloques se logra mediante el enlace secuencial y cronológico de los bloques, utilizando el hash del bloque anterior que se almacena en el encabezado de cada bloque (Rahardja, Hidayanto, Lutfiani, Febiani, & Aini, 2021, pág. 4). Esta conexión crea una estructura similar a una cadena, de donde proviene el nombre *blockchain.* Este enlace criptográfico asegura que sea computacionalmente inviable alterar un bloque sin modificar también todos los bloques posteriores en la cadena, garantizando así la integridad de toda la cadena (Rahardja, Hidayanto, Lutfiani, Febiani, & Aini, 2021, págs. 4-5).

B. Concepto de nodo

Otro aspecto fundamental para poder entender cómo funciona la tecnología *blockchain* es comprender como funcionan los mecanismos de consenso que proporcionan esa seguridad y validación de los distintos bloques de la cadena. Antes de poder explicar esto con detalle, se va a explicar la anatomía de la cadena. Para ello, se debe entender la cadena de bloques como una red distribuida entre usuarios, que a nivel técnico se conocen como nodos. Los nodos más comunes son los que se conocen como nodos completos, que se encargan de almacenar la totalidad de la *blockchain.* Cuando se realiza una transacción, estos nodos son utilizados para comprobar si la transacción es válida, ya que al contener la totalidad de la cadena sirve de fuente fiable para comparar (Nakamoto, 2008, pág. 4). Gracias a ellos, se consigue combatir la propagación de transacciones inválidas.

Otro tipo de nodo son los nodos ligeros o *SPV (Simple Payment Verification),* que se encargan de almacenar únicamente la cabecera del resto de bloques. Este tipo es de gran utilidad si se quiere acceder a la red con dispositivos con menor capacidad computacional, como puede ser un dispositivo móvil (Nakamoto, 2008, pág. 9).

C. Mecanismos de consenso

Una vez ya explicado los nodos básicos de la red, se va a analizar los diferentes mecanismos de consenso que existen dentro de esta tecnología. Estos protocolos son fundamentales para que los diferentes nodos participantes lleguen a un acuerdo sobre el estado de la *blockchain*. Los mecanismos que se van a estudiar en este análisis van a ser el PoW y el PoS, ya que son los más utilizados en la actualidad. Algunos de los otros mecanismos son el PoA y el PBFT, que a pesar de ser protocolos correctos no se implementan tan a menudo.

El mecanismo de prueba de trabajo (Proof of Work)[1] es uno de los más usados en la actualidad debido a ser uno de los originales en la creación de la tecnología. El principio en el que se basa es en exigir a los nodos participantes de la red que resuelvan complejas operaciones matemáticas para poder validar las transacciones y que sean incluidas en la *blockchain*. En este caso, se suele referirse a los nodos que realizan estas operaciones como nodos mineros (Vikas & Satpalsing , 2020, págs. 1-2). La forma de proceder es la siguiente (Nakamoto, 2008, pág. 3):

[1] En adelante referido como PoW.

En primer lugar, el minero encuentra la solución a la operación matemática; luego, difunde la solución a la red y el resto de los nodos se encargan de verificar la operación. Una vez verificada, se añade a la cadena de todos los nodos, y finalmente se recompensa al nodo minero.

Gracias a esta forma de proceder, se asegura la seguridad y la descentralización del protocolo, ya que el coste computacional de controlar más de la mitad de la cadena es extremadamente costoso, y debido a la descentralización cualquier persona puede ser partícipe de la cadena. El principal argumento detractor de este mecanismo de consenso es el alto coste computacional que requiere los cálculos matemáticos y de forma consecuente el alto consumo de energía que este conlleva. De ahí a que esta forma de proceder sea vista de forma negativa en términos de su impacto medioambiental. Otros argumentos en contra de este protocolo son sus problemas de escalabilidad al irse incrementando la complejidad de las operaciones matemáticas, que llevan a un mayor tiempo de procesamiento por transacción. Esta cuestión lleva también al uso de tecnología cada vez más potente que puede llevar a la formación de centros de minería que comprometen la descentralización de la red (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, págs. 3-4). Algunas de las redes más conocidas que implementan este mecanismo son Bitcoin, Ethereum, ZCash y Monero entre otras muchas, aunque la que implementa de forma más pura este protocolo es la red creada por Satoshi Nakamoto.

El siguiente mecanismo que se va a detallar es la prueba de participación (Proof of Stake)[2], teorizado por primera vez en 2011 en un foro de Bitcoin como alternativa al PoW. Para poder implementar este protocolo es necesario que exista una criptomoneda nativa asociada (*tokens)* y en él, los participantes se consideran todos validadores de las transacciones y utilizan el capital que poseen de la criptomoneda nativa como contraprestación para poder confirmar las operaciones. Esto se conoce como *staking*. La forma de obtener consenso en este mecanismo está basada en turnos entre los validadores, que van proponiendo y votando el siguiente bloque candidato a formar parte de la cadena. La selección del siguiente validador está basado en la aleatoriedad y en la cantidad de *staking* de cada validador.

Las principal ventaja de PoS es la gran eficiencia energética significativamente mayor en comparación con el PoW, ya que no requiere una potencia computacional intensiva para

[2] En adelante referido como PoS.

la minería. Generalmente también ofrece tiempos de procesamiento de transacciones más rápidos y un mayor rendimiento que el PoW. Tiene barreras de entrada más bajas para los participantes, ya que no necesita hardware especializado costoso, y cualquier persona que posea la cantidad requerida de criptomoneda puede convertirse en validador. También puede conducir a una mejor escalabilidad en comparación con el PoW debido a no tener un factor limitante de cálculo como tiene el PoW (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 4).

Sin embargo, existe un riesgo potencial de centralización si un pequeño número de grandes poseedores de *tokens* acumulan una cantidad significativa de participación, lo que les otorga una influencia desproporcionada sobre la red. El modelo de seguridad, aunque robusto, está menos probado en batalla en comparación con la larga historia del PoW. Los sistemas PoS pueden ser susceptibles al problema de "nada en juego", donde los validadores podrían estar incentivados a votar en múltiples cadenas en conflicto, ya que no hay un costo significativo por hacerlo. Las recompensas para los validadores podrían ser más bajas en comparación con las recompensas de bloque en los sistemas PoW (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 4).

Ejemplos exitosos que implementan de forma satisfactoria este mecanismo es Cardano, fundada por uno de los cofundadores de Ethereum, que implementa el protocolo Ourobourous PoS garantizando un retorno de entre el 5% y el 7% a sus usuarios. Otras *blockchains* de éxito que integran este protocolo son Solana, Algorand y Polkadot (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 5).

Cabe mencionar la existencia de DPoS o prueba de participación delegada, una variante del PoS. En este protocolo, los poseedores de *tokens* dentro de la red votan para elegir un conjunto más pequeño de delegados (también conocidos como testigos o productores de bloques) que luego son responsables de validar las transacciones y producir nuevos bloques en la *blockchain*. Este mecanismo tiene como objetivo combinar los beneficios de la participación de los interesados con la eficiencia de un conjunto de validadores más pequeño (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 5).

El DPoS generalmente logra tiempos de procesamiento de transacciones más rápidos y un mayor rendimiento en comparación con PoW y PoS tradicional debido al número limitado de validadores activos. Es más eficiente energéticamente que PoW, ya que no implica una minería intensiva. Puede ofrecer una mejor escalabilidad en comparación con

PoW y algunas implementaciones de PoS. Incorpora un elemento democrático a través del proceso de votación, permitiendo a los poseedores de *tokens* influir en la selección de validadores. El proceso de votación continuo permite la eliminación de delegados con bajo rendimiento o maliciosos (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 5).

Sin embargo, aunque tiene como objetivo la descentralización, el DPoS aún puede enfrentar riesgos de centralización si un pequeño número de delegados dominan constantemente el proceso electoral. El poder de voto a menudo es proporcional a la cantidad de *tokens* que se poseen, lo que puede llevar a la influencia de grandes interesados. Mantener la responsabilidad de los delegados depende de la participación activa e informada de los poseedores de *tokens*, y la apatía de los votantes puede ser un desafío. Como en toda red descentralizada, existe la posibilidad de que los delegados formen cárteles o conspiren, comprometiendo la integridad de la red (Katiyar, Verma, Kumar, Kumar, & Sahu, 2023, pág. 5).

3. Principales plataformas y ecosistemas (Bitcoin, Ethereum, etc.)

Bitcoin y Ethereum se destacan como las dos plataformas *blockchain* más prominentes e influyentes, sirviendo como pilares de los ecosistemas de criptomonedas y aplicaciones descentralizadas. Bitcoin y Ethereum son, sin lugar a duda, las principales criptomonedas y han desempeñado un papel significativo en el desarrollo de la industria criptográfica. Ether (ETH), la criptomoneda nativa de la red Ethereum, es el segundo *token* digital más popular después de bitcoin (BTC) y la segunda criptomoneda más grande por capitalización de mercado. Bitcoin y Ethereum han marcado hitos significativos en la evolución de las finanzas digitales, introduciendo al mundo los conceptos de *blockchain* y finanzas descentralizadas (DeFi). Vamos ahora a profundizar con mayor detalle en estas dos plataformas para tener un mejor entendimiento del estado del arte actual.

A. Bitcoin

El protocolo fundacional de Bitcoin se explica como un sistema de efectivo electrónico de igual a igual. Bitcoin se propuso en un *whitepaper* publicado por Satoshi Nakamoto en 2008 como el primer sistema de pago electrónico basado en una red descentralizada de igual a igual, eliminando la necesidad de un tercero de confianza. Este tenía como

objetivo resolver los problemas relacionados con el anonimato, la descentralización, la ausencia de confianza y la transparencia en las transacciones digitales, permitiendo a los pares realizar transacciones directamente sin intermediarios (Nakamoto, 2008). La idea central era crear un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, permitiendo que dos partes dispuestas realizaran transacciones directamente. En el ya citado *whitepaper*, Nakamoto estableció la estructura básica de la red Bitcoin y presentó la idea de una criptomoneda descentralizada. El diseño de Bitcoin enfatiza un sistema de igual a igual, de computadora a computadora, en lugar de a través de un servidor central o intermediario.

La estructura de la red sigue el patrón ya descrito en apartados anteriores: los bloques están formados por encabezados y por cuerpo. Dentro de los bloques el sistema almacena una cantidad limitada de transacciones que unidas al resto de transacciones incluidas en los bloques restantes de la cadena dan lugar a la totalidad de la *blockchain*. La red de Bitcoin utiliza el mecanismo de PoW como protocolo de consenso. En él, los mineros realizan el esfuerzo computacional que supone resolver el problema criptográfico que se les suele plantear para poder validar una transacción. El parámetro que establece la dificultad de la prueba es el *nonce*, que se encuentra dentro del encabezado de cada bloque (Nakamoto, 2008). Profundizando más en la arquitectura de Bitcoin, vemos que tanto la seguridad como la descentralización son una prioridad. Para la primera, el PoW y el enlace criptográfico de los bloques asegura una seguridad robusta. Como contrapartida, tenemos el elevado consumo energético que estos cálculos conlleva. En la actualidad, para poder conseguir una mejor eficiencia se hace uso de tarjetas gráficas o GPU que tienen una capacidad de cómputo muy superior a las CPU de los ordenadores actuales.

Tal como se describe en el *whitepaper,* la idea detrás de Bitcoin es la creación de una moneda digital segura y resistente a la censura que puedan forzar los bancos centrales. Esta resistencia a la posible censura se consigue gracias a la descentralización que esta posee, ya que la red no está vinculada a ninguna autoridad estatal que sea responsable de validar o no las transacciones realizadas (Rasul, 2018, pág. 2). Bitcoin pretende ser una forma de gobernanza algorítmica pura basada en una red de voluntarios iguales entre ellos que implementan de forma colectiva un libro de contabilidad. Debido a la descentralización sobre la que está diseñada, la red se considera realmente segura desde el punto de vista de ciberseguridad. Esto se da al no existir puntos únicos de fallo que colapsen la red si no están disponibles.

Una de las características principales de Bitcoin es que tiene un suministro fijado por defecto de 21 millones de *tokens* en toda la red. Esto supone un cambio de paradigma en el sistema fiduciario, ya que en nuestra economía los bancos centrales controlan la emisión de dinero con el fin de regularla. Al haber un oferta limitada, esto puede llevar a que su valor incremente con el tiempo, característica común entre los activos deflacionarios. En la actualidad, se ha "minado" cerca del 90% del suministro total de la moneda (Fabus, Kremenova, Stalmasekova, & Kvasnicova-Galovicova, 2024, pág. 1). Para poder continuar con la emisión y aumentar su escasez, el protocolo está diseñado para ir recompensando con menor cantidad de criptomoneda a los mineros. Este proceso se conoce como *halving* ya que cada cuatro años se reduce a la mitad la recompensa obtenida por bloque minado. En su génesis, cada bloque minado beneficiaba a su minero con 50 BTC; en 2012 se redujo a 25, hasta la actualidad que recompensa cada bloque minado con 3,125 BTC. De esta forma, se estima que en el 2140 se habrán minado la totalidad del suministro (Fabus, Kremenova, Stalmasekova, & Kvasnicova-Galovicova, 2024, pág. 2) .

En la actualidad y a fecha de redacción del documento, Bitcoin cotiza en el mercado secundario a 83.101,42 €. Esto supone una revalorización desde su emisión de casi un 21.000% (Google Finance, 2024). La escasez inherente de Bitcoin, impulsada por su oferta fija, y su naturaleza descentralizada lo posicionan como una posible reserva de valor digital. Esta escasez, junto con su control descentralizado, resuena con las características de los activos refugio tradicionales como puede ser el oro. Sin embargo, su volatilidad de precios sigue siendo un desafío para la adopción generalizada como reserva de valor estable. Las constantes fluctuaciones de precios, como lo demuestran varios eventos del mercado y análisis de volatilidad, indican que su estabilidad como reserva de valor aún está evolucionando, como cabe esperar de una tecnología naciente.

B. Ethereum

La red Ethereum se ha consolidado como una plataforma líder dentro del ecosistema *blockchain*, trascendiendo su concepción inicial como una mera criptomoneda para convertirse en una infraestructura fundamental para una amplia gama de aplicaciones descentralizadas (*dApps)*. La concepción inicial de Ethereum se atribuye a Vitalik Buterin, quien a finales de 2013 plasmó su visión en un documento fundacional: el

whitepaper de Ethereum. Este trabajo propuso una "plataforma de contratos inteligentes y aplicaciones descentralizadas de próxima generación", marcando una ambición que iba mucho más allá de las funcionalidades ofrecidas por Bitcoin en aquel momento. Buterin anunció formalmente el inicio del proyecto Ethereum en enero de 2014, durante la North American Bitcoin Conference (Buterin, 2014). En esta etapa temprana, figuras clave como Gavin Wood se unieron al proyecto, desempeñando un papel crucial en la definición de la especificación técnica de la Máquina Virtual de Ethereum (EVM) a través del influyente Yellow Paper (Wood, 2014). La financiación inicial para el desarrollo de Ethereum se obtuvo a través de una oferta inicial de monedas (ICO) en 2014. La visión de Buterin se distinguió por su enfoque en la creación de una *blockchain* programable, capaz de ejecutar una amplia variedad de aplicaciones descentralizadas, a diferencia del enfoque principal de Bitcoin como moneda digital *peer-to-peer*.

A lo largo de su historia, el proyecto de Buterin ha pasado por múltiples fases de desarrollo. La red se lanzó de forma oficial en el año 2015 bajo el nombre clave “Frontier”. En esta primera iteración, los usuarios de la plataforma podían minar la criptomoneda nativa, conocida como Ether (ETH), usando PoW como mecanismo de consenso, de forma similar a la red Bitcoin. Esta fase se caracteriza por la introducción de los smart contracts, programas autoejecutables almacenados en los bloques de la red encargados de automatizar la ejecución de acuerdos, que resultan vitales para desarrollar aplicaciones descentralizadas (Gopan, 2023, pág. 4). Esta primera fase no se consideraba definitiva, pero con el lanzamiento de “Homestead” en 2016 se consiguió la primera versión estable de la plataforma, superando la fase experimental en la que se encontraba. En julio de este mismo año sucedió un evento clave para la red: la organización DAO (Decentralised Autonomous Organization), un *venture capital* descentralizado construido sobre Ethereum, sufrió un hackeo por parte de un grupo no reconocido que resultó en un robo de 3,6 millones de Ether, la moneda nativa, que en ese momento suponía alrededor de 50 millones de dólares (Staff, 2025). Este suceso abrió en un debate sobre cómo responder a este tipo de ataques que se zanjó con una escisión dentro de la red en dos nuevas cadenas: Ethereum (la nueva y objeto de estudio) y Ethereum Classic (la original) (Staff, 2025).

En los años posteriores, se fueron introduciendo mejoras en la red que supusieron un incremento en la escalabilidad de la *blockchain*. No fue hasta 2022 cuando se introdujo uno de los mayores cambios en la red: una transición de PoW a PoS como mecanismo de

consenso. Esta transición se llevó a cabo en lo que se conoce como "The Merge", la integración de una cadena independiente que usaba PoS con la cadena ya existente de Ethereum. De esta forma, se instauró la prueba de participación como mecanismo de consenso oficial dentro de la cadena. El gran incentivo para este cambio fue la mejora sustancial de eficiencia energética, que se estima en 99,95%. En esta transición, los mineros fueron reemplazados por validadores y el proceso de *staking* se instauró para asegurar la red (Solmonte, 2023, págs. 14-15). En el año 2023, se introduzco una mejora haciendo posible que los validadores pudieran retirar su ETH de *staking,* mejorando la flexibilidad de la red.

En cuanto a la composición de la red, en esta los bloques también tienen encabezado y cuerpo del bloque. El cuerpo del bloque contiene lo mismo que los bloques de Bitcoin: el conjunto de las transacciones de la red. La gran diferencia radica en el contenido del encabezado: en él, encontramos nuevos campos como son el *gasLimit* y *gasUsed*, que miden tanto la energía máxima permitida para minar ese bloque como la cantidad realmente utilizada (Jezek, 2020, pág. 13). Otros campos nuevos son *beneficiary*, que hace referencia al usuario recompensado, o el campo *extraData* para almacenar metadata de menor relevancia. Con el fin de tener un almacenamiento eficiente y seguro, Ethereum implementa diferentes versiones de los árboles Merkle Patricia (MPT) para almacenar información sobre el estado de la red. Debido a ello, en el encabezado encontramos campos como *stateRoot o transactionsRoot,* que almacenan punteros a la raíz de los árboles que almacenan tanto el estado global de todas las cuentas como el de todas las transacciones. Al organizarse de esta forma, la búsqueda de información dentro de la *blockchain* resulta significativamente más rápida que de otras formas (Jezek, 2020, pág. 13).

La gran diferencia de la *blockchain* de Ethereum con Bitcoin reside en los contratos inteligentes[3]. Este concepto fue introducido por Nick Szabo en 1994 y hace referencia a programas autoejecutables que eliminan la necesidad de intermediarios al introducir mecanismos transparente y seguros que ejecuta los acuerdos (Gopan, 2023, pág. 4). El *software* encargado de ejecutar estos *smart contracts* es la Ethereum Virtual Machine (EVM). Este programa actúa en el fondo de la cadena de manera autónoma en un entorno seguro y aislado, y va ejecutando los diferentes contratos de las *dApps* (Gopan, 2023, pág.

[3] En adelante referidos como *smart contracts*.

3). Gracias a este servicio, los desarrolladores han sido capaces de crear aplicaciones descentralizadas para ofrecer servicios en distintos sectores. Algunos de los casos de éxito son Uniswap en el intercambio de *tokens*, protocolos de préstamos de liquidez como Aave y mercados de *tokens no fungibles* (NFT) como OpenSea o CryptoPunks. Para poder implementar estas *dApps,* los desarrolladores se acogen al estándar ERC-20 de creación de *tokens*. Este se trata de un conjunto de reglas y funciones estandarizadas que permiten que exista interoperabilidad dentro del ecosistema de Ethereum (Victor & Lüders, 2018, pág. 3).

III. Régimen jurídico

1. Panorama internacional y organismos reguladores

La rápida expansión de nuevas fórmulas de financiación basadas en tecnología *blockchain* (emisión de criptoactivos mediante *ICOs*, *security tokens*, plataformas de DeFi, etc.) ha impulsado a los reguladores a elaborar un marco jurídico específico.

A nivel internacional no existe una regulación unificada de los criptoactivos; sin embargo, diversos organismos y foros globales han emitido directrices para coordinar las políticas nacionales. Por ejemplo, la Organización Internacional de Comisiones de Valores (IOSCO) publicó en 2023 un conjunto de 18 recomendaciones para establecer estándares globales en la regulación de criptomonedas y activos digitales (Shine, 2024). Asimismo, el Consejo de Estabilidad Financiera (*Financial Stability Board*, FSB), por encargo del G20, elaboró en 2023 un marco regulatorio global con recomendaciones de alto nivel para la supervisión consistente de los mercados de criptoactivos. Dichas recomendaciones se basan en el principio de *"mismo riesgo, misma regulación"*, buscando mitigar la volatilidad intrínseca y riesgos sistémicos de estos activos. No obstante, estas pautas internacionales se centran en riesgos financieros (estabilidad, protección inversor) y reconocen que aún no abarcan todos los riesgos específicos, como algunos asociados a las plataformas DeFi puras (Release, 2023).

Las aproximaciones regulatorias varían significativamente por país. En Estados Unidos, por ejemplo, aún no se ha aprobado una ley federal integral sobre criptoactivos pese a propuestas debatidas en el Congreso (como la *Ley de Innovación Financiera del Siglo XXI*); la regulación allí se ha basado en la aplicación de leyes de valores o *commodities* existentes, generando cierta inseguridad jurídica (Shine, 2024). En contraste, jurisdicciones como Reino Unido han avanzado marcos propios: toda empresa que ofrezca servicios con criptomonedas en el Reino Unido debe estar autorizada por la Financial Conduct Authority (FCA), incluso si opera desde el extranjero (Shine, 2024), y se han propuesto reglas específicas para *stablecoins* y otras criptoactividades. Por otro lado, algunos países han optado por restricciones severas (China prohibió la operativa con criptomonedas en 2021), mientras que otros han favorecido la adopción (El Salvador otorgó curso legal al bitcoin en 2021, aunque esta medida ha sido cuestionada por organismos como el FMI). En síntesis, el panorama mundial sigue siendo heterogéneo,

pero con una clara tendencia hacia mayores exigencias regulatorias coordinadas a nivel internacional.

2. Legislación y directivas europeas (MiCA, entre otras)

La Unión Europea se ha posicionado como pionera a nivel global al establecer el primer marco normativo integral sobre criptoactivos. En mayo de 2023 se aprobó el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, conocido como MiCA (*Markets in Crypto-Assets*), que introduce reglas uniformes para los emisores de criptoactivos no cubiertos por la normativa financiera tradicional y para los proveedores de servicios sobre criptoactivos (MiCA, 2023). MiCA tiene por objeto cerrar el vacío regulatorio existente hasta entonces en la UE: antes de MiCA, muchos *tokens* no encajaban en las categorías jurídicas de los instrumentos financieros o dinero electrónico, quedando fuera de supervisión. El reglamento abarca la emisión, oferta pública y admisión a negociación de criptoactivos, así como la prestación de servicios relacionados (intercambio, custodia, asesoramiento en criptoactivos, etc.), estableciendo requisitos de transparencia, divulgación de información, autorización y supervisión tanto para emisores como para intermediarios (MiCA, 2023). Se incluyen normas de protección del inversor (p. ej. obligación de publicar un libro blanco con información clara antes de una oferta pública) y medidas contra abusos de mercado en criptoactivos (prohibición de manipulación de mercado e *insider trading*).

Bajo la regulación MiCA, los activos conocidos como *stablecoins* se dividen en dos categorías según sus distintos mecanismos de respaldo: en ARTs y en EMTs. El primero de ellos, los ARTs, son aquellos que su valor está respaldado por múltiples activos. Un ejemplo de ART es Libra, que hacía un seguimiento del dólar estadounidense, del euro, del yen japonés, la libra esterlina y el dólar singapurense. La otra categoría son las EMTs, que son aquellas cuyo valor está respaldado por un único activo. El caso más notable de EMT es Tether, la criptomoneda que replica el valor del dólar estadounidense.

Es importante destacar que los criptoactivos considerados *security tokens* o *NTF* no están contemplados en el ámbito regulatorio del reglamento MiCA

3. Regulación en España: CNMV, Banco de España y normativa aplicable

En España, el tratamiento jurídico de la financiación mediante *blockchain* ha evolucionado rápidamente, pasando de un vacío normativo a un marco en plena adaptación a MiCA. Antes de la aprobación de MiCA, no existía una regulación específica de los criptoactivos en el ordenamiento español: las llamadas "criptomonedas" no eran reconocidas como medio de pago legal, ni contaban con el respaldo de ninguna autoridad pública, ni estaban cubiertas por mecanismos de protección al cliente, como el Fondo de Garantía de Depósitos o el Fogain para inversores (España, 2021, pág. 1). Las autoridades financieras españolas - la Comisión Nacional del Mercado de Valores (CNMV) y el Banco de España - advirtieron reiteradamente a los inversores sobre estos hechos y sobre los elevados riesgos de volatilidad y fraude asociados a los criptoactivos. Asimismo, dejaron claro que hasta la fecha ninguna oferta de criptomoneda o ICO había sido registrada o autorizada en España, dado que muchos criptoactivos no encajaban en las categorías financieras existentes y por tanto escapaban a la supervisión tradicional. En ausencia de normativa sectorial específica, se aplicaba la normativa general según el caso: por ejemplo, si un criptoactivo confería derechos económicos equivalentes a valores negociables (e.g. acciones, participaciones en beneficios, derechos de voto), podría ser considerado un instrumento financiero y, en tal caso, quedaría sujeto a la Ley del Mercado de Valores y regulaciones europeas de valores (MiFID II, Folleto, etc.) al igual que cualquier otro valor (Garcia-Fuentes, 2024). De hecho, la CNMV ha aclarado que un criptoactivo puede ser jurídicamente un instrumento financiero si cumple las características legales (independientemente de que utilice *blockchain*), y de ser así, debe regirse por las mismas reglas que los valores tradicionales. Esta interpretación sentó las bases para distinguir entre "utility *tokens*" no regulados y "security *tokens*" sometidos a supervisión de la CNMV bajo la normativa de valores.

Con la llegada de MiCA, España ha tomado varias medidas para adaptar su marco legal y dotar de base institucional a la nueva regulación. Mediante la Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión (LMVSI), el legislador designó expresamente a la CNMV y al Banco de España como autoridades competentes en materia de criptoactivos (Moncloa, 2023). En concreto, la CNMV fue nombrada autoridad supervisora para la emisión, oferta pública y admisión a negociación de

criptoactivos que no tengan la consideración de instrumentos financieros, anticipando así la aplicación de MiCA en España (Garcia-Fuentes, 2024). Por su parte, el Banco de España asumirá la supervisión, inspección y potestad sancionadora en lo referente a las obligaciones de los emisores de *tokens* referenciados a activos (ART) y de dinero electrónico (EMT) bajo MiCA, dada su afinidad con las funciones tradicionales del banco central (CNMV, s.f.). Esta distribución de competencias CNMV/Banco de España quedó consagrada en la LMVSI de 2023 y asegura una coordinación interinstitucional: la CNMV vigilará los aspectos de mercado e inversores, mientras el Banco de España controlará los aspectos prudenciales de las *stablecoins*.

Durante el periodo intermedio hasta la plena implantación de MiCA, las autoridades españolas han implementado medidas provisionales para controlar la actividad de criptomercados. Desde 2021, el Banco de España mantiene un registro oficial de proveedores de servicios de criptomonedas (cambio de moneda virtual por fiduciaria y custodia de monederos electrónicos), en el que deben inscribirse todas las empresas que ofrezcan estos servicios en España (CNMV, s.f.). Dicha obligación – establecida inicialmente con fines de prevención de blanqueo de capitales – ha servido para tener un censo y supervisión básica de *exchanges* y custodios mientras entra en vigor MiCA. Los proveedores registrados en este registro del Banco de España podrán seguir operando de forma transitoria hasta finales de 2025, pero deben obtener autorización de la CNMV bajo MiCA para continuar más allá de esa fecha (finReg360, 2024).

En cuanto a la publicidad y protección al inversor, España fue uno de los primeros países en regular específicamente la promoción de criptoactivos. La CNMV, amparada por el Real Decreto-ley 5/2021, emitió la Circular 1/2022 para someter a control administrativo la publicidad de criptoactivos ofrecidos como inversión. Esta normativa obligaba a que los anuncios fueran claros, equilibrados y no engañosos, e introducía la exigencia de notificar previamente a la CNMV las campañas publicitarias masivas sobre criptomonedas, incluyendo mensajes estandarizados de advertencia sobre riesgos (FinReg360, 2024). Gracias a esta iniciativa, cualquier anuncio dirigido al público español debía informar, por ejemplo, de que “las inversiones en criptoactivos no están reguladas, pueden no ser adecuadas para inversores minoristas y se puede perder la totalidad del importe invertido”. Sin embargo, tras la entrada en vigor de MiCA, que contiene *directamente* reglas uniformes para la publicidad en toda la UE, la CNMV decidió derogar la Circular 1/2022 para evitar duplicidades. Mediante la Circular 1/2024,

publicada el 27 de diciembre de 2024, se suprimió la normativa nacional de publicidad cripto con efecto desde el 28 de diciembre de 2024, dado que MiCA ya exige publicidad imparcial y faculta a la CNMV a intervenir anuncios cuando sea necesario (FinReg360, 2024).

IV. Concepto y Emisión de *Tokens*

1. Definición y tipología de *tokens* (utility, security, stablecoins, NFTs, etc.)

La palabra *token* deriva de la palabra "tacen" del inglés antiguo, que hace referencia a un símbolo o un signo. Se utiliza comúnmente para referirse a objetos especiales similares a monedas, emitidos de forma privada y con un valor intrínseco insignificante, como fichas de transporte, fichas de lavandería y fichas de juegos recreativos. (Antonopoulos, 2019, Capítulo 10)

Hoy en día, los *tokens* gestionados mediante cadenas de bloques están redefiniendo el término, pasando a significar abstracciones basadas en *blockchain* que pueden poseerse y que representan activos, monedas o derechos de acceso. (Antonopoulos, 2019, Capítulo 10). Los *tokens* de *blockchain*, en su esencia, no poseen una definición intrínseca única, sino que funcionan principalmente como herramientas para el intercambio de valor dentro de la cadena de bloques. Este proceso de transformación, conocido como tokenización, implica la encapsulación de activos digitales o del mundo real, asignándoles una representación digital negociable en la *blockchain* (Marin, Cioara, Toderean, Mitrea, & Anghel, 2023, pág. 7). A diferencia de las criptomonedas, que son el activo nativo de una *blockchain*, como Bitcoin, los criptoactivos se construyen sobre *blockchain*s existentes, como Ethereum, utilizando plantillas estandarizadas como el estándar ERC-20 (Mansa & Rosenton, 2024).

Estos *tokens* se utilizan con frecuencia para la recaudación de fondos en proyectos, siendo creados, distribuidos, vendidos y circulados a menudo a través de un proceso de Oferta Inicial de Monedas (ICO). Pueden servir como inversiones, para almacenar valor o para realizar compras dentro de sus respectivos ecosistemas (Mansa & Rosenton, 2024). La seguridad de los criptoactivos se garantiza mediante diversas técnicas criptográficas, incluyendo algoritmos de cifrado, pares de claves públicas-privadas y funciones de hash, como ya se ha explicado en apartados anteriores. Los contratos inteligentes[4] son fundamentales para procesar y gestionar las transacciones de *tokens*, automatizando los acuerdos y eliminando la necesidad de intermediarios

[4] En adelante *smart contracts.*

Una vez contextualizado, se va a proceder a la categorización de los diferentes tipos de *tokens* que se encuentran en la actualidad.

A. Tokens de utilidad o utility tokens.

Los *tokens* de utilidad están diseñados para proporcionar a los usuarios acceso a características, servicios o productos específicos dentro de una plataforma basada en *blockchain*, funcionando como una forma de moneda interna. Facilitan las operaciones de un mercado descentralizado, cubren tarifas de transacción o participan en la gobernanza de una organización o sistema descentralizado (Marin, Cioara, Toderean, Mitrea, & Anghel, 2023, pág. 7). A diferencia de los *tokens* de seguridad, los *tokens* de utilidad no otorgan participaciones de propiedad en una empresa ni derechos a la participación en beneficios. Su valor se deriva de la funcionalidad que ofrecen dentro de la plataforma asociada, vinculándose directamente a la demanda de los servicios o productos del ecosistema *blockchain*. Son fundamentales para el funcionamiento de las aplicaciones descentralizadas (*dApps*) y pueden influir en las tarifas de transacción, los derechos de voto o la disponibilidad de servicios dentro del ecosistema.

Los *tokens* de utilidad se crean durante las Ofertas Iniciales de Monedas (ICOs) o los Eventos de Generación de *Tokens* (TGEs) para financiar el desarrollo de proyectos (Kumar Sharma, 2025). Uno de los detractores de los *utility tokens* es la mención recurrente de su uso en ICOs para recaudar fondos, que revela una tensión inherente. Su valor idealmente debería depender de su utilidad real, pero en la práctica, su valoración inicial y la especulación a menudo están ligadas al éxito de la recaudación de fondos y al *hype* del mercado (Kumar Sharma, 2025). Esta dualidad presenta un desafío regulatorio significativo: cómo diferenciar un *token* que es puramente funcional de uno que, de facto, opera como una inversión, especialmente dada la historia de estafas asociadas con las ICOs. Esto explica la postura de MiCA, que exige transparencia para los *tokens* de utilidad, pero con normas menos estrictas que para las *stablecoins*, reconociendo su función principal, pero mitigando riesgos.

Uno de los casos de uso más notables es Filecoin, donde los usuarios pagan por servicios de almacenamiento utilizando los *tokens* de la plataforma. Esa capacidad de almacenamiento que se busca es proporcionada por los mineros.

B. Tokens de seguridad o security tokens

Los *tokens* de seguridad son representaciones digitales de activos, instrumentos y derechos económicos (como bienes inmuebles, propiedad intelectual o participación en ingresos) encapsulados en un formato tokenizado digital. Pueden utilizarse de manera similar a los valores tradicionales para pagar dividendos, compartir beneficios o conceder derechos de voto (Group, 2024, pág. 5). Representan la propiedad o la inversión en una empresa. A diferencia de los valores electrónicos convencionales que se gestionan en un servidor central, los valores tokenizados tienen sus libros de transacciones compartidos entre los participantes en una red *blockchain*, lo que proporciona transparencia y seguridad a los inversores. Se crean mediante Ofertas de *Tokens* de Seguridad (STOs). Los poseedores de *security tokens* tienen derechos legales asociados a la propiedad. Su valor tiende a ser más estable y menos especulativo en comparación con los *tokens* de utilidad, ya que a menudo está vinculado al rendimiento de activos tangibles (Group, 2024, págs. 5-6).

Los *tokens* de seguridad están respaldados por activos tangibles y se adhieren a marcos regulatorios, lo que los convierte en una opción más segura y regulada que las ICOs. El Reglamento MiCA excluye explícitamente los *security tokens* de su ámbito directo si ya están regulados por la normativa de instrumentos financieros existente, como MiFID II (MiCA, 2023). La Autoridad Europea de Valores y Mercados (ESMA) tiene el mandato de emitir directrices sobre las condiciones y criterios para la calificación de los criptoactivos como instrumentos financieros, con el fin de aclarar la delimitación entre los ámbitos de aplicación de MiCA y MiFID II (ESMA, 2024, pág. 17).

Un ejemplo de *security tokens* en España es la compañía Reental SL, una empresa norteamericana que posee una plataforma de inversión inmobiliaria basada en la tokenización. En su caso, este proceso se basa en la captación del valor de dicho inmueble y su división en distintas fracciones. Mediante su plataforma, el inversor particular puede invertir en bienes inmuebles con poco capital, que no serían accesibles de otra forma. Además, ofrece liquidez en la inversión ya que el inversor puede desinvertir en cualquier momento ofreciendo sus *tokens* al mercado (Sánchez, 2023).

C. Stablecoins

Las stablecoins son criptomonedas cuyo valor está vinculado a monedas fiduciarias o a otros activos. Son unidades digitales de valor que utilizan herramientas de estabilización para mantener un valor constante en relación con una o varias monedas oficiales u otros activos (incluidos los criptoactivos) (Adachi, Mitsu, 2022, pág. 1). Su desarrollo surgió para abordar las altas fluctuaciones de precios de los criptoactivos no respaldados, como Bitcoin y Ethereum, y su baja volatilidad las hace adecuadas para funciones que requieren estabilidad de precios. Buscan servir como medio de liquidación para productos financieros automatizados y ofrecen posibilidades de "dinero programable" (Adachi, Mitsu, 2022, pág. 2).

MiCA regula las stablecoins, clasificándolas en dos categorías principales: *Tokens* Referenciados a Activos (ARTs) si referencian el valor de múltiples activos, y *Tokens* de Dinero Electrónico (EMTs) si están vinculadas al valor de una única moneda fiduciaria de curso legal, como el euro (MiCA, 2023). El reglamento impone requisitos estrictos para las *stablecoins*, incluyendo requisitos de reserva, gobernanza y reglas de estabilización. Eventos de inestabilidad, como los ocurridos con la criptomoneda Luna, demostraron que las *stablecoins* pueden no ser tan estables como se percibe, destacando los posibles canales de contagio de riesgos financieros debido a su vínculo directo con el sector financiero tradicional a través de sus activos de reserva (Adachi, Mitsu, 2022). La Autoridad Bancaria Europea (EBA) proporciona directrices sobre los requisitos de información para los emisores de ARTs y EMTs bajo MiCA, buscando asegurar la convergencia supervisora y un enfoque común en los Estados Miembros. Las normas sobre ARTs y EMTs entraron en vigor antes que el resto de MiCA, el 30 de junio de 2024.

Una de las *stablecoins* de referencia en la actualidad es Tether, que mantiene una paridad 1:1 con el dólar estadounidense. Funciona de la siguiente manera: los usuarios depositan dinero en las cuentas de la empresa emisora, Tether Limited, y reciben como contrapartida el mismo valor depositado en USDT, la *stablecoin* en cuestión.

D. *Tokens* no fungibles o *NTFs*

Los *Tokens* No Fungibles (NFTs) son un tipo de registro digital de propiedad que se utiliza de manera única para garantizar la autenticidad y la singularidad de un activo. A diferencia de los *tokens* fungibles (como las criptomonedas o los *tokens* de utilidad), cada NFT es único e insustituible, lo que les confiere una propiedad de escasez digital inherente (Pereira, Ferreira, & Quintino, 2022, pág. 1). Son fundamentalmente transformadores en el proceso de comercialización de activos digitales. Debido a sus características únicas, los NTFs se han utilizado en diversos mercados como los juegos o el arte digital, ya que representan activos únicos como puede ser un determinado "item" en un juego o una obra de arte.

El Reglamento MiCA excluye explícitamente los NFTs de su ámbito de aplicación general, ya que representan activos únicos (MiCA, 2023). Sin embargo, la regulación establece una excepción importante: si los NFTs se emiten de forma fraccionada y esas fracciones son fungibles entre sí, podrían entrar bajo el ámbito de MiCA. Esto indica que la fungibilidad, incluso si se deriva de la fragmentación de un activo no fungible, puede activar la supervisión regulatoria de MiCA (MiCA, 2023).

En la actualidad, la obra digital llamada "Everydays: The First 5000 Days" fue subastada por casi 70 millones de dólares estadounidenses, en un evento celebrado por Christie's en marzo de 2021. La obra se compone de diversas imágenes que muestran el desarrollo artístico que ha ido experimentando el creador a lo largo de los 5.000 días que duró el proyecto (Beeple, 2021).

2. Modelos de financiación a través de *tokens*: ICO, STO, IEO, IDO

Una vez explicada el concepto de *token* y los principales tipos que están presentes en la actualidad, se va a proceder a una descripción de los diferentes modelos de financiación que siguen los distintos proyectos. Varias de estas se han mencionado en apartados anteriores, lo que denota la presencia que estas formas tienen en la actualidad. Existen múltiples formas de obtener la financiación necesaria, pero vamos a centrarnos en las más importantes: ICO, STO, IEO e IDO.

A. Oferta Inicial de Moneda o *Initial Coin Offer (ICO)*

Las Ofertas Iniciales de Monedas (ICOs) son un mecanismo de crowdfunding en el que se crean, distribuyen, venden y circulan criptoactivos con el propósito de recaudar fondos para proyectos. Este modelo surgió como una forma atractiva de captar capital, principalmente debido a sus costos reducidos en comparación con los métodos de financiación tradicionales (Group, 2024, pág. 7). Un componente central del proceso de ICO es el "whitepaper", un documento técnico exhaustivo que detalla los objetivos del proyecto, el equipo, las especificaciones técnicas y la estrategia de distribución de *tokens* (Shi, 2024, pág. 2).

Entre las ventajas de las ICOs se encuentran su alta liquidez, el potencial de un alto retorno de la inversión, su amplia disponibilidad para inversores globales, la rapidez del proceso de recaudación de capital y la minimización de los costos asociados (Šapkauskienė & Višinskaitė, 2020, pág. 4). Los *tokens* adquiridos en una ICO suelen cotizar en plataformas virtuales en un plazo de tres meses, lo que proporciona liquidez a los inversores. Algunos proyectos lograron recaudar capital a velocidades récord; por ejemplo, Gnosis obtuvo 12 millones de dólares en menos de 10 minutos, y Bancor atrajo 150 millones de dólares en solo tres horas. Proyectos como Tezos, EOS y Filecoin (que recaudó aproximadamente 4.300 millones de dólares, marcando una de las campañas de crowdfunding más exitosas) son ejemplos de ICOs que lograron captar fondos sustanciales (Šapkauskienė & Višinskaitė, 2020, pág. 5).

Por otra parte, las ICOs también presentan desventajas significativas. Se caracterizan por altos riesgos debido a la asimetría de información, la falta de protección del inversor y una regulación adecuada (Šapkauskienė & Višinskaitė, 2020, pág. 2). La historia de estas está marcada por una alta frecuencia de estafas y actividades fraudulentas; en 2017, se estimó que cuatro de cada cinco ICOs eran fraudes. La ausencia de una supervisión regulatoria robusta y de requisitos de diligencia debida expuso a los inversores a riesgos considerables. En ausencia de una diligencia debida regulatoria formal, el *whitepaper* se convirtió en el documento principal para que los inversores evaluaran un proyecto de ICO (Šapkauskienė & Višinskaitė, 2020, pág. 2). Esto sugiere que, en un mercado no regulado, los mecanismos informales de divulgación de información intentan llenar la brecha de confianza. Sin embargo, la prevalencia de *whitepapers* replicados y sitios web de proyectos falsificados indica que este mecanismo a menudo era insuficiente o fácilmente manipulable. Esto implica que, si bien se desea la transparencia, los marcos regulatorios

formales suelen ser necesarios para garantizar la calidad y la veracidad de la información divulgada, especialmente cuando hay un capital significativo involucrado.

B. Oferta de Tokens de Seguridad o Security Tokens Offer (STO)

Las Ofertas de *Tokens* de Seguridad (STOs) representan un método para que las empresas recauden capital mediante la venta de *tokens* digitales que representan la propiedad o la inversión en su negocio. Se consideran una opción más segura y regulada que las ICOs, ya que se adhieren a marcos regulatorios y están respaldadas por activos tangibles (Group, 2024, pág. 5). La programabilidad a través de *smart contracts* permite funciones automatizadas como la distribución de dividendos, los derechos de voto y las comprobaciones de cumplimiento, lo que simplifica las operaciones y minimiza las tareas administrativas.

Las STOs ofrecen múltiples beneficios para la captación de capital y la liquidez. Proporcionan acceso a capital global, mayor liquidez (especialmente para activos tradicionalmente ilíquidos como bienes raíces y arte), transacciones más rápidas y económicas (gracias a los contratos inteligentes), mayor transparencia y cumplimiento, y la posibilidad de propiedad fraccionada (Melashych, 2025). La mayor liquidez de los *tokens* de seguridad podría reducir los períodos mínimos de inversión, ya que los inversores pueden intercambiar sus *tokens* en mercados secundarios.

Este modelo de financiación representa la "evolución regulada" de la financiación con *tokens*, actuando como un puente entre las finanzas tradicionales y digitales. Su adhesión a las leyes de valores existentes le otorga credibilidad, lo que a su vez atrae a una base más amplia de inversores, incluidos los institucionales, que suelen ser reacios a los mercados no regulados (Group, 2024, pág. 9). Esto implica que la conformidad regulatoria es un factor clave para la adopción generalizada de la financiación basada en *blockchain*, especialmente para la tokenización de activos del mundo real.

C. Oferta Inicial de Intercambio o *Initial Exchange Offer (IEO)*

Las Ofertas Iniciales de Intercambio (IEOs) son un método de recaudación de fondos en el que un proyecto vende sus *tokens* directamente en un *exchange* de criptomonedas, con

el *exchange* actuando como intermediario (Furnari, 2021, pág. 10). A diferencia de las ICOs, las IEOs implican un *exchange* externo que realiza la diligencia debida del proyecto, lo que mejora la credibilidad y ayuda a filtrar estafas y proyectos de baja calidad. Los *exchange*s suelen proporcionar un entorno más seguro para los inversores, incluyendo el cumplimiento de KYC (Conoce a tu Cliente) y AML (Anti-Lavado de Dinero) (Furnari, 2021, pág. 10).

Las IEOs ofrecen varias ventajas. Proporcionan una mayor confianza debido a la participación de un *exchange* de buena reputación, un proceso simplificado para los inversores (quienes pueden comprar *tokens* fácilmente con sus cuentas de *exchange* sin necesidad de configurar *wallets*), acceso inmediato al mercado (aprovechando la base de usuarios existente del *exchange*) y liquidez inmediata (los *tokens* se listan poco después de la venta) (Furnari, 2021, pág. 12). Sin embargo, también presentan desventajas, como las tarifas del *exchange* (que reducen los fondos recaudados), un control limitado del proyecto sobre el proceso de recaudación de fondos y el potencial de un mayor escrutinio regulatorio (Furnari, 2021, págs. 12-13).

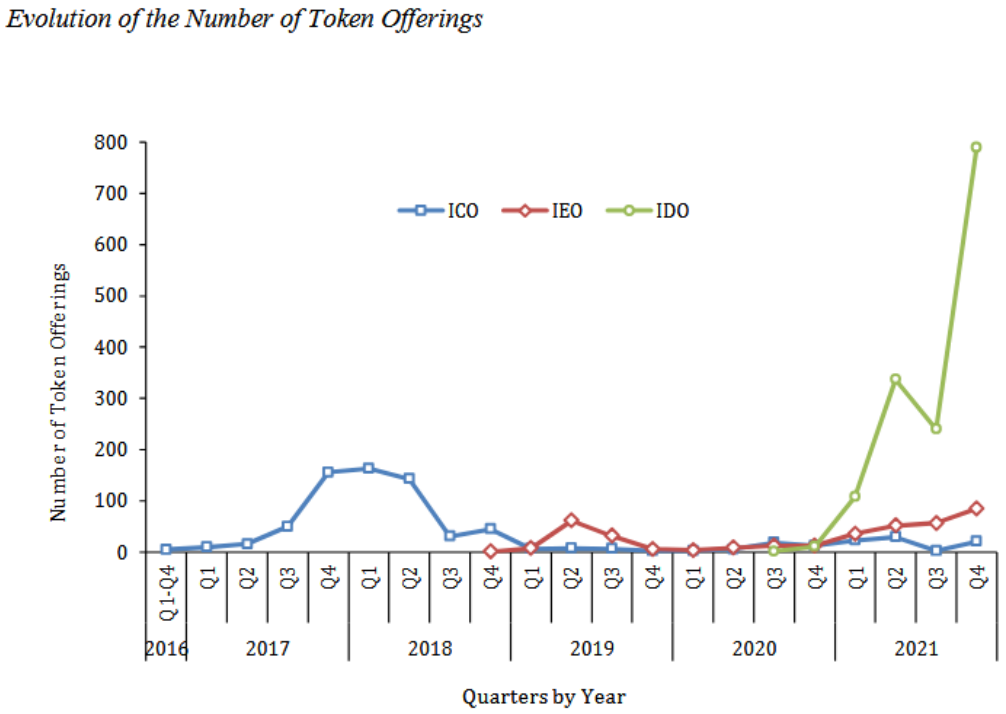
El auge de las IEOs sigue directamente la "pérdida de confianza" en las ICOs, aprovechando explícitamente la reputación de los *exchanges* centralizados (CEXs) para verificar proyectos y proporcionar protección al inversor (Furnari, 2021, pág. 14). Esto representa un cambio pragmático: aunque *blockchain* promueve la descentralización, el mercado buscaba un modelo de financiación más fiable, incluso si eso significaba reintroducir un intermediario. La relación causal es que la alta tasa de fraude de las ICOs llevó a una demanda de mayor verificación, que los CEXs estaban en posición de proporcionar (Furnari, 2021, págs. 14-15).

D. Oferta Inicial de DEX o *Initial DEX Offer (IDO)*

Las Ofertas Iniciales de DEX (IDOs) son un método de recaudación de fondos que utiliza exchanges descentralizados (DEXs) para lanzar nuevos proyectos de criptomonedas. La principal diferencia que tiene con las IEOs es que operan directamente en plataformas descentralizadas, lo que garantiza un entorno sin confianza, sin permisos y descentralizado, eliminando intermediarios. En lugar de contar con una entidad centralizada encargada de regular, son los contratos inteligentes los que gestionan la

distribución de *tokens* y el procesamiento de pagos, automatizando el proceso. (Magnusson & Renhage, 2022, págs. 45-46).

Figura 1. Evolución de la forma de financiación



Fuente: (Magnusson & Renhage, 2022, pág. 45)

En la figura siguiente se puede ver la evolución que han tenido los principales métodos de financiación en los últimos años. El descenso de los ICOs se ve explicado por la desconfianza que este método provoca en los inversores, que ven que sus inversiones no tienen seguridad. Para paliar este miedo, el mercado comenzó a pivotar hacia soluciones más seguras y reguladas como las IEOs y las IDOs.

Las IDOs representan la "re-descentralización" de la financiación con *tokens*, enfatizando los sistemas sin confianza. Tras la intermediación centralizada de las IEOs, las IDOs vuelven al tema central de la *blockchain* de la descentralización, eliminando a los exchanges centralizados como guardianes. Esto hace ver la existencia de una búsqueda continua del equilibrio óptimo entre eficiencia, confianza y descentralización en la

recaudación de fondos (Magnusson & Renhage, 2022, págs. 49-50). La relación causal es que el deseo de evitar el control centralizado y las tarifas/escrutinio asociados impulsa el desarrollo de mecanismos de financiación verdaderamente descentralizados. Esto implica un compromiso filosófico dentro de partes de la comunidad cripto con los sistemas sin confianza, incluso si reintroduce parte del riesgo para el inversor visto en las primeras ICOs debido a la falta de supervisión (Magnusson & Renhage, 2022, págs. 49-50).

3. Factores clave en la emisión (*tokenomics*, liquidez, gobernanza)

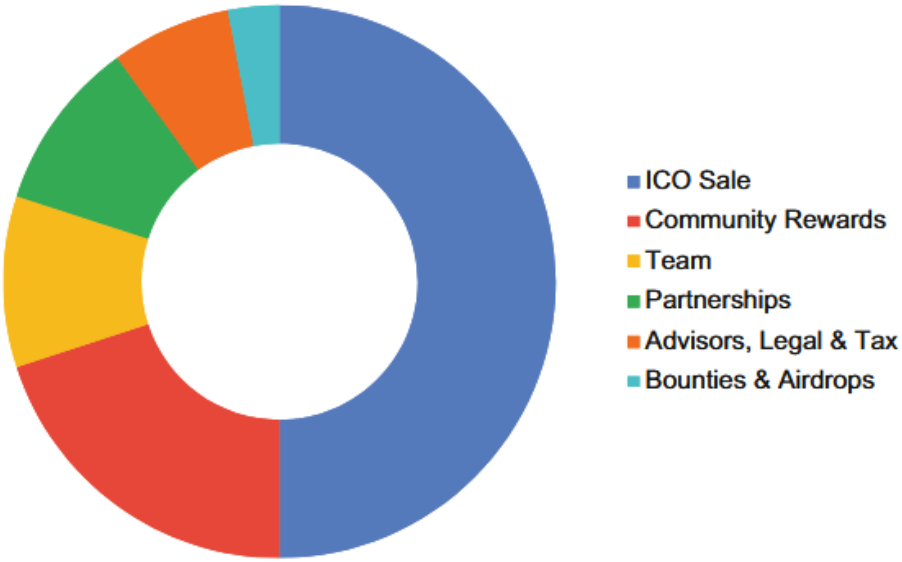
Una vez explicado con detalle el concepto de *token* y los diferentes mecanismos que las empresas y proyectos tienen para financiarse, se van a explicar los aspectos clave que determinan la emisión de un *token*. Estos factores son la clave para asegurar la visibilidad, el valor y el éxito de los proyectos a largo plazo. *Tokenomics*, liquidez y gobernanza conforman un círculo virtuoso que influye directamente en la atracción de capital y la legitimidad ante los reguladores.

A. Tokenomics

El concepto *tokenomics* hace referencia a la economía de un *token.* Dentro de esta economía, destacan una serie de pilares fundamentales: su suministro total, su suministro circulante, mecanismos de distribución y los diferentes procesos inflacionarios o deflacionarios que sufre a lo largo del tiempo (Wandmacher, 2019, pág. 113). El suministro total es el número máximo de *tokens* que se van a emitir y no siempre ha de ser limitado. Casos como los de Ethereum con su moneda ETH, que no tiene un límite, se contraponen a otros como los 21 millones de BTC que la red de Bitcoin emitirá. La fijación de un suministro total es una de las estrategias que los diferentes proyectos pueden usar para impulsar la demanda y el valor, a costa de perder flexibilidad para responder a demandas del mercado. Estrategias como los modelos inflacionarios que no tienen un suministro total fijo ofrecen mayor flexibilidad y atraen a inversores en busca de recompensas. De forma contraria, los modelos deflacionarios se basan en la disminución progresiva de la oferta mediante mecanismos como la "quema" de *tokens*, que no es más que una eliminación de cierta parte del suministro circulante. Este método es la contrapartida del "*minting*", es decir, la creación de nuevos *tokens.*

En cuanto a la distribución de los *tokens* de la red, no todos son emitidos en una ICO o similar. Normalmente, la red emisora guarda un porcentaje de los *tokens* para otras funciones, como la recompensa a la comunidad, para el equipo de desarrollo y *airdrops*[5], entre otras cosas (Wandmacher, 2019, pág. 117). En la figura siguiente, se puede observar la distribución normal que siguen los proyectos.

Figura 2. Reparto del suministro



Fuente: (Wandmacher, 2019, pág. 6)

En definitiva, *tokenomics* no trata solo de cifras, sino de diseñar incentivos y desincentivos que moldeen el comportamiento del usuario, la participación en la red y, en última instancia, la viabilidad y el valor a largo plazo de un proyecto.

B. Liquidez

La liquidez es una ventaja fundamental de la financiación de los *tokens*, ya que permite a los inversores recuperar rápidamente su capital y obtener rendimientos de estos. La tecnología *blockchain* mejora la transparencia de las transacciones, reduciendo de esta forma el riesgo de contraparte y permitiendo una toma de decisiones más ágil. Otras

[5] Un *airdrop* es una estrategia de distribución gratuita de *tokens* o criptomonedas entre un grupo específico o generalizado de usuarios, con el fin de aumentar la visibilidad, adopción y descentralización del proyecto, premiando a usuarios específicos por ciertas acciones.

características como la inmutabilidad de los registros o la descentralización de los datos son catalizadores de una mejora en la eficiencia operativa. Esta mejora consigue reducir los períodos mínimos de inversión, ya que los inversores tienen flexibilidad a la hora de vender sus activos (Laurent, Chollet, Burke, & Seers, 2019, pág. 2).

Si bien la alta liquidez se presenta como una ventaja importante para los inversores (rendimientos rápidos, salida fácil), existen preocupaciones sobre la estabilidad en un mercado hiperlíquido y riesgos de *hacking*. Esto sugiere que, si bien la liquidez es deseable, una liquidez excesiva o no regulada puede introducir nuevas formas de inestabilidad y vulnerabilidad del mercado. La implicación es que la búsqueda de la máxima liquidez debe equilibrarse con medidas de seguridad sólidas y supervisión regulatoria para prevenir la manipulación del mercado, las caídas repentinas u otros riesgos sistémicos que pueden surgir de un comercio rápido y sin restricciones

C. Gobernanza

En el contexto de los *tokens,* la gobernanza hace referencia a la forma en la que se toman las distintas decisiones dentro de un proyecto o ecosistema. Para ello, existen lo que se conocen como *tokens* de gobernanza, que otorgan derechos de voto a los poseedores de los activos y les permiten participar en la toma de decisiones dentro de la *blockchain,* basándose en las reglas especificadas en los *smart contracts* (Qunie, 2024, pág. 7). Dado que uno de los principios fundamentales de la tecnología *blockchain* es la descentralización, la mayoría de los proyectos se basan en una gobernanza descentralizada como se ha descrito anteriormente.

A menudo, la gobernanza en la cadena de bloques se concibe en tres capas: la comunidad *off-chain,* que engloba a los desarrolladores y mineros, el desarrollo *on-chain,* que hace referencia a los diferentes cambios que se hacen mediante un proceso de voto, y los protocolos *on-chain* (Polcumpally, Kumar, Kumar, & Samadhiya, 2024, págs. 10-11). Existen varios modelos de implementación, incluyendo plataformas *off-chain* como Snapshot, arquitecturas de gobernanza híbridas y sistemas de delegación basados en *tokens*, cada uno con ventajas y desventajas en términos de transparencia, costo y adaptabilidad. Si bien el ideal es la gobernanza descentralizada, los fragmentos de información reconocen la existencia de la comunidad *off-chain*, el desarrollo *off-chain* y las arquitecturas de gobernanza híbridas. Esto sugiere que la gobernanza puramente *on-*

chain y basada en *tokens* a menudo es insuficiente o impráctica para todas las decisiones, lo que lleva a una combinación de mecanismos *on-chain* y *off-chain,* como los explicados previamente (Polcumpally, Kumar, Kumar, & Samadhiya, 2024, pág. 11).

V. Creación y Emisión de un *Token*

1. Elección de la plataforma

La elección de la plataforma *blockchain* óptima representa un paso inicial fundamental en cualquier proyecto, que exige una evaluación equilibrada de la funcionalidad, la adaptabilidad y la compatibilidad con los productos de software existentes. Las plataformas se clasifican generalmente en públicas frente a privadas, y de propósito general frente a específicas de aplicación, siendo esencial comprender su arquitectura subyacente y sus capacidades para seleccionar la tecnología de libro mayor distribuido adecuada para una aplicación específica (Banoo Muradi & Kia Chim, 2022).

Ethereum ha emergido como una opción predominante para el desarrollo de contratos inteligentes. Posee el ecosistema y la comunidad de desarrolladores más grandes y activos, lo que ha fomentado un vasto conjunto de herramientas de código abierto y marcos de desarrollo. Esta riqueza de recursos reduce significativamente la necesidad de que los desarrolladores construyan desde cero, generando un efecto de red que amplifica el valor general de la red (Che, Xia, & Lo, 2021, pág. 5). Desde su lanzamiento en 2015, Ethereum se ha consolidado como la *blockchain* habilitada para contratos inteligentes más madura, demostrando una notable estabilidad en miles de empresas y casos de uso, y superando numerosas actualizaciones de protocolo.

La Máquina Virtual de Ethereum (EVM) es un componente central que admite múltiples lenguajes de programación, principalmente Solidity y Vyper, lo que la hace accesible para desarrolladores con diversos niveles de experiencia (Che, Xia, & Lo, 2021, pág. 7). Solidity, en particular, inspirado en JavaScript y lenguajes de la familia C, es ampliamente utilizado para la implementación de contratos inteligentes en Ethereum. Además de estos lenguajes de programación, Ethereum ofrece un sólido conjunto de herramientas y marcos de desarrollo, como Truffle, Hardhat, Remix IDE, Ganache, Web3.js, Ethers.js y OpenZeppelin, que simplifican el proceso de desarrollo de aplicaciones descentralizadas (*dApps*), desde la creación y compilación de contratos hasta las pruebas y el despliegue (Kobusinska & Wilczynski, 2022, pág. 3).

La evolución de Ethereum ilustra una dinámica crucial en el espacio *blockchain*: el "volante de la madurez, la seguridad y el ecosistema". Una red madura atrae a más desarrolladores, lo que a su vez impulsa la creación de más aplicaciones y herramientas.

Este ecosistema en expansión y el desarrollo continuo mejoran la estabilidad y la seguridad percibida de la red, que a su vez genera un potente efecto de red que consolida la posición de Ethereum como plataforma líder de contratos inteligentes, a pesar de la competencia (Huang & Wang, 2021).

2. Estructura básica de un contrato inteligente (*Smart Contract*) y definición de sus funciones

Hasta este momento, se ha descrito de forma breve qué es un contrato inteligente pero no se ha profundizado en la estructura ni en cómo se crea uno. Antes de entrar a esto, es imprescindible entender de forma adecuada el concepto que hay detrás de ellos. Un contrato inteligente o *smart contract* es un programa autoejecutable que reside en la *blockchain* de Ethereum. Estos están principalmente escritos en Solidity, un lenguaje de programación similar a JavaScript, y son ejecutados sobre la EVM de Ethereum. Cada nodo de la red ejecuta la EVM, por lo que se garantiza que el mismo comportamiento para todos y sus resultados son verificados por todos, lo que guarda el principio de descentralización que posee la red.

En términos de estructura, los *smart contracts* suelen tener partes comunes a todos. En primer lugar, encontramos las variables de estado que son todos los datos almacenados permanentemente en la *blockchain*, como el balance de *tokens*. A continuación, encontramos la parte importante, que son las funciones. En ellas se encuentra la lógica que define el contrato y suelen ser o bien públicas o privadas, dependiendo de si son para uso interno o han de ser ejecutadas al recibir una transacción. Lo siguiente son los eventos, que no son más que mecanismos que se encargan de registrar y emitir información durante la ejecución del contrato para que clientes externos pueden ver qué se está ejecutando. Finalmente, se encuentran los modificadores, que establecen las condiciones para que se ejecuten las diferentes funciones, y el constructor, una función especial que se ejecuta automáticamente al desplegar el contrato para inicializar su estado.

A continuación, tenemos un ejemplo de la forma que sigue un *smart contract*:

Figura 3. Ejemplo de smart contracts

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

/// @title Ejemplo de Smart Contract
/// @notice Implementación del estándar ERC-20 (EIP-20), con mint y burn.

contract EjemploERC20Educativo {
    // --- Datos del token ---
    string public name = "Token de Ejemplo";       // Nombre del token (opcional)
    string public symbol = "MTE";                  // Símbolo (opcional)
    uint8  public decimals = 18;                   // Decimales habituales (opcional)

    uint256 private _totalSupply;                  // Suministro total interno

    // Mapping de balances: dirección => saldo
    mapping(address => uint256) private _balances;

    // Mapping de allowances: owner => (spender => cantidad autorizada)
    mapping(address => mapping(address => uint256)) private _allowances;

    // --- Eventos según EIP-20 ---
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);

    // --- Funciones obligatorias ERC-20 (EIP-20) ---

    /// @notice Cantidad total de tokens en existencia.
    function totalSupply() external view returns (uint256) {
        return _totalSupply;
    }

    /// @notice Saldo de `account`.
    function balanceOf(address account) external view returns (uint256) {
        return _balances[account];
    }

    /// @notice Transfiere `amount` tokens de `msg.sender` a `to`.
    function transfer(address to, uint256 amount) external returns (bool) {
        require(to != address(0), "ERC20: transfer a cero");
        require(_balances[msg.sender] >= amount, "ERC20: saldo insuficiente");

        // Actualiza balances
        _balances[msg.sender] -= amount;
        _balances[to] += amount;

        emit Transfer(msg.sender, to, amount);
        return true;
    }

   /// @notice Permite que `spender` gaste hasta `amount` de los tokens de `msg.sender`.
    function approve(address spender, uint256 amount) external returns (bool) {
        require(spender != address(0), "ERC20: approve a cero");

        _allowances[msg.sender][spender] = amount;
        emit Approval(msg.sender, spender, amount);
        return true;
    }

    /// @notice Transfiere `amount` tokens de `from` a `to`, usando allowance.
     function transferFrom(address from, address to, uint256 amount) external returns
(bool) {
       require(from != address(0) && to != address(0), "ERC20: transferencia invalida");
```

```
62.         require(_balances[from] >= amount, "ERC20: saldo insuficiente");
63.                 require(_allowances[from][msg.sender] >= amount, "ERC20: allowance
insuficiente");
64.
65.         // Actualiza allowance y balances
66.         _allowances[from][msg.sender] -= amount;
67.         _balances[from]          -= amount;
68.         _balances[to]            += amount;
69.
70.         emit Transfer(from, to, amount);
71.         return true;
72.     }
73.
74.     /// @notice Cantidad que `spender` puede gastar de `owner`.
75.     function allowance(address owner, address spender) external view returns (uint256)
{
76.         return _allowances[owner][spender];
77.     }
78.
79.     // --- Extensiones educativas: mint y burn ---
80.
81.     /// @notice Crea `amount` tokens y los asigna a `to`.
82.     /// @dev En un contrato real habría un control de acceso (owner/minter).
83.     function mint(address to, uint256 amount) external {
84.         require(to != address(0), "mint a cero");
85.
86.         _totalSupply           += amount;
87.         _balances[to]          += amount;
88.
89.         emit Transfer(address(0), to, amount);
90.     }
91.
92.     /// @notice Destruye `amount` tokens del saldo de `msg.sender`.
93.     function burn(uint256 amount) external {
94.         require(_balances[msg.sender] >= amount, "burn: saldo insuficiente");
95.
96.         _balances[msg.sender]  -= amount;
97.         _totalSupply           -= amount;
98.
99.         emit Transfer(msg.sender, address(0), amount);
100.    }
101. }
102.
```

Fuente: Elaboración propia a partir de datos de ejemplo de una IA

En primer lugar, tenemos la cabecera, donde se define el protocolo que se va a seguir, a la vez que el compilador que se va a usar (líneas 1-2). A continuación, tenemos datos del *token* (líneas 7-11), como su nombre, símbolo y número de decimales que tendrá este para representar su valor. Se suele utilizar 18 para poder dividir el *token* en unidades muy pequeñas.

A partir de la línea 13, encontramos las variables de estado del contrato, las cuales persisten en la cadena de bloques. La variable *_totalSupply* (línea 13) es un *uint256* que almacena el suministro total de *tokens* que existen. Está declarada como variable privada para evitar que sea modificada directamente, garantizando la integridad de su valor a través de funciones controladas.

Las siguientes variables son *mappings* (líneas 16 y 19), estructuras de datos clave-valor similares a los diccionarios o hash tables en otros lenguajes de programación. El *mapping* *_balances* (línea 16) asocia cada dirección (*address*) con su saldo de *tokens* (*uint256*), lo que permite al contrato llevar un registro de cuántos *tokens* posee cada usuario. El *mapping* anidado *_allowances* (línea 19) es una pieza clave para la funcionalidad de *transferFrom*. Almacena las autorizaciones de gasto, donde un dueño (owner) permite que un (*spender*) gaste una cantidad (*amount*) específica de sus *tokens* en su nombre.

El código define dos eventos (líneas 22-23), *Transfer* y *Approval*, que son fundamentales para la transparencia del contrato. Un evento es una forma de que el contrato comunique información a la red Ethereum y a las aplicaciones externas. Una vez que se emiten (función *emit*()), los eventos son almacenados en los logs de la transacción y no pueden ser modificados. Los *exchanges*, *wallets* y otros servicios de la Web3 utilizan estos eventos para monitorear los movimientos de los *tokens* y actualizar el saldo de los usuarios.

El estándar ERC-20 exige la implementación de varias funciones públicas. La función *totalSupply()* (líneas 28-30) devuelve el suministro total del *token*, mientras que *balanceOf()* (líneas 33-35) devuelve el saldo de una dirección específica. Ambas son funciones *view*, lo que significa que no modifican el estado de la cadena y no consumen gas (Buterin, 2014).

La función *transfer()* (líneas 38-48) permite a los usuarios enviar *tokens* de su propio saldo a otra dirección. Contiene dos validaciones *require* (líneas 39-40) que garantizan que el destinatario no sea una dirección nula, *address(0),* y que el emisor tenga saldo suficiente. Si ambas condiciones se cumplen, los saldos se actualizan y se emite el evento *Transfer*.

La función *approve()* (líneas 51-57) autoriza a un tercero (*spender*) a gastar una cantidad específica de *tokens* en nombre del *msg.sender*. Esta autorización se registra en el *_allowances mapping*. Por otro lado, la función *transferFrom()* (líneas 60-72) ejecuta la transferencia en nombre del dueño original, siempre que exista una autorización previa. Ambas funciones incluyen validaciones estrictas y emiten sus respectivos eventos al completarse (Buterin, 2014).

Finalmente, la función *allowance()* (líneas 75-77) permite consultar la cantidad de *tokens* que un *spender* tiene permiso para transferir de una dirección específica (Buterin, 2014).

3. Proceso de testeo y despliegue en la red

El desarrollo de aplicaciones descentralizadas (*dApps*) y la subsiguiente emisión de *tokens*, como se ha explorado en las secciones previas de este estudio, culminan en una de las fases más críticas y de mayor responsabilidad: el proceso de testeo y despliegue en una red *blockchain*. Esta etapa no se limita a ser un mero procedimiento técnico, sino que representa la validación final de la seguridad, la funcionalidad y la viabilidad de todo el proyecto. La principal razón de esta criticidad reside en la naturaleza fundamental de la tecnología de los contratos inteligentes: su inmutabilidad una vez que han sido desplegados en la red principal, *Mainnet* (Wilson, 2025). Un error de codificación, una vulnerabilidad de seguridad o un fallo en la lógica de negocio, si se detectan post-despliegue, pueden acarrear consecuencias irreversibles, incluyendo la pérdida irrecuperable de fondos, la manipulación del sistema o una erosión total de la confianza de la comunidad.

El principio de inmutabilidad de la *blockchain*, aunque una fortaleza, también es un arma de doble filo que hace que las pruebas y auditorías sean críticas. El ataque a The DAO en 2016, donde un fallo en un contrato inteligente permitió robar 60 millones de dólares en Ether, evidenció esta vulnerabilidad, generando una crisis que llevó a la bifurcación de Ethereum en Ethereum y Ethereum Classic, como ya se ha explicado con detalle en apartados anteriores. Este evento impulsó a la industria a desarrollar metodologías y herramientas rigurosas, convirtiendo la seguridad y las pruebas en una necesidad existencial para los proyectos de tokenización, más que una simple práctica recomendada.

El proceso comienza con la preparación del entorno de desarrollo. La elección del *framework* es estratégica y existen diversas opciones en la actualidad: Hardhat destaca por su flexibilidad y herramientas de depuración avanzadas, mientras que Truffle es una suite más madura y "todo en uno". Por otro lado, Foundry ofrece un enfoque minimalista que permite escribir pruebas directamente en Solidity, el lenguaje nativo de la red Ethereum.

Una vez configurado correctamente el entorno, se procede a realizar pruebas diferentes pruebas exhaustivas. En primer lugar, se considera buena práctica de los programadores el realizar tests unitarios para cada parte nueva de código que producen. En estos tests, el programador define como se debe comportar el código dado una serie de información de

entrada. A continuación, se realizan pruebas de integración que verifican que las interacciones entre los distintos contratos de la red funcionan de forma correcta. Finalmente, se realiza una verificación formal usando reglas lógicas y matemáticas con el fin de demostrar que el código se adhiere a una especificación concreta. El enfoque que se persigue con tanta diligencia a la hora de testear es tratar de romper el funcionamiento del programa y encontrar todos los fallos del código antes de que entre en producción.

Siguiendo la metodología empleada durante la fase de pruebas, los contratos se despliegan primero en redes de prueba como Goerli o Sepolia, que son réplicas de la red principal que no tienen *token*s con valor monetario (Wilson, 2025). Para poder desplegar los nuevos contratos, se usan plataformas como Infura o Alchemy, en colaboración con carteras Web3 como MetaMask para poder firmar las diferentes transacciones. Aun con el objetivo de descentralizar la *blockchain*, el proceso de despliegue suele depender de nodos centralizados, como los servicios de RPC (Remote Procedure Call) que proporciona Infura y Alchemy. Esto genera un potencial punto de fallo que compromete los principios fundamentales por los que se rige la red. Por ello, se han comenzado a desarrollar alternativas descentralizadas como DIN (Descentralizad Infrastructure Network), que pretenden solventar esta problemática.

4. Costes de gas, seguridad y mejores prácticas

Las "gas fees" son las tarifas que se pagan para ejecutar transacciones y operaciones en la red de Ethereum, remunerando a los validadores por su trabajo y asegurando la red [37, 38]. Desde la implementación de la EIP-1559, actualización de la red en el año 2021, el cálculo de la tarifa total (gas fee) se ha simplificado y se compone de dos elementos principales: una tarifa base (base fee), que es un cantidad retirada de la circulación por el protocolo, y una propina (priority fee), que se paga opcionalmente al validador para incentivar la inclusión de la transacción en un bloque. La tarifa total se calcula mediante la siguiente fórmula (Metamask, 2025):

$$(base\_fee + priority\_fee)\ x\ unidades\ de\ gas\ utilizadas$$

Resulta de vital importancia diferenciar el límite de gas, que es la cantidad máxima de unidades de gas dispuesta a pagar por una transacción, y el precio del gas, que se define como el costo por unidad de gas. Esto resulta de interés cuando hablamos de que una

transacción se “queda sin gas”. Esto quiere decir que el límite de gas establecido para completar la transacción fue insuficiente para completar la transacción (Stein, 2025).

La optimización del gas tiene más implicaciones aparte de la reducción de costes, ya que influye en la escalabilidad y el rendimiento que tendrá el proyecto. Existen diferentes prácticas que permiten a los proyectos tener un mejor desempeño. En primer lugar, minimizar el uso del almacenamiento permanente (*storage)* y usar en su lugar la memoria volátil *(memory)* permite que las operaciones sean más rápidas. Otra de las técnicas más eficientes es agrupar las diferentes operaciones en lotes para poder reducir el coste total, ya que las transacciones a menudo requieren de operaciones externas para poder completarse (NadlabAdmin, 2025).

Finalmente, la auditoria de un contrato inteligente busca identificar problemas de seguridad y de eficiencia que no ha podido ser identificado durante el período de testeo realizado con anterioridad. Las dos vulnerabilidades más comunes son: ataques de reentrada, que son contratos maliciosos que interfieren con la ejecución del contrato y puede drenar los fondos de las cuentas implicadas en un contrato. Un ejemplo notorio de esta vulnerabilidad es el incidente del The DAO (QuillAuditsAdmin, 2025).

La otra vulnerabilidad es el desbordamiento de enteros durante las operaciones aritméticas. Esto se puede producir durante la ejecución de las operaciones dentro de la transacción, donde una operación supera el valor máximo permitido por el contrato y el protocolo reinicia el valor de esa variable a un valor por defecto. Los atacantes usan esta debilidad para manipular los saldos de las cuentas para poder obtener más *token*s de los que les corresponden. El ejemplo más sonado de este caso es el ataque a PoWHCoin (Banisadr, 2018)

VI. Casos de Estudio

1. Tokenización de Instrumentos Financieros

Como se ha explicado en apartados anteriores, la tokenización es el proceso de crear una representación digital de un activo físico o financiero dentro de una cadena de bloques. Gracias a este proceso, está comenzado a ser cada vez más común que activos tradicionalmente ilíquidos, como los bienes raíz, sean divididos en fracciones y negociados en mercados secundarios especializados. La inclusión de estos proyectos está ayudando a reducir la barrera de entrada para inversores y a aumentar drásticamente la liquidez. Los activos más tokenizados son las acciones, los bonos y la deuda, y otros productos como los fondos de inversión o derivados financieros.

La tokenización de acciones permite la propiedad fraccionada y desliga a los inversores de depender del horario de apertura y cierre de los diferentes mercados bursátiles. Además de esto, elimina la necesidad de intermediarios tradicionales ya que no existe un organismo centralizado que tenga que validar la operación, sino que es la propia red la que se encarga de solucionarlo. El caso de la plataforma tZERO, que tokenizó las acciones de Overstock.com, es un ejemplo pionero de cómo la *blockchain* puede crear un mercado secundario para acciones tokenizadas. Según un informe del CFA Institute (Soni, Fines, & Sun, 2025), se destaca que la tokenización de acciones mejora la eficiencia operativa, reduce los periodos de bloqueo de capital y amplía el espectro de inversión mínima requerida.

Por otro lado, el sector de la tokenización de bonos y deuda se considera uno de los de mayor potencial dentro de las finanzas descentralizadas. Este potencial reside en la reducción de costes de emisión y los tiempos de liquidación, y la automatización de los pagos de intereses a través de los *smart contracts*. Según el informe publicado por el BIS (Aldasoro, y otros, 2025), los bonos tokenizados ya tienen costes de emisión y *bid-ask spreads*[6] más bajos que los bonos convencionales, a pesar de encontrarse en una fase incipiente. A pesar de estas ventajas, esta tecnología sufre los mismos problemas que hemos visto a lo largo del documento.

[6] El *bid-ask spread* es la diferencia que existe entre el valor máximo (*bid)* que un comprador está dispuesto a pagar y el mínimo valor (*ask)* al que el vendedor está dispuesto a vender. Una diferencia pequeña indica que el activo es líquido.

Finalmente, existen casos donde se ha utilizado para tokenizar fondos de inversión y derivados financieros. Firmas como Franklin Templeton han tokenizado fondos de bonos gubernamentales, utilizando la *blockchain* de Ethereum para ofrecer a los inversores participaciones tokenizadas con transferencias en tiempo real y mayor liquidez. La tokenización de derivados, como futuros y opciones, permite la creación de activos sintéticos, lo que reduce el riesgo de contraparte y aumenta la eficiencia y transparencia del mercado. El caso de HSBC y su *Token* de Oro en Hong Kong, que permite a los inversores minoristas adquirir una participación fraccionada en oro físico, es un ejemplo de la tokenización de activos reales tangibles (HSBC, 2024).

2. Proyectos con controversias legales o sanciones

La rápida evolución de la financiación mediante *blockchain* no ha estado exenta de controversias significativas que han puesto a prueba los límites del marco regulatorio existente. El análisis de ciertos casos emblemáticos permite ilustrar la aplicación práctica de los principios jurídicos discutidos y las consecuencias derivadas de su incumplimiento, sirviendo como catalizadores para el desarrollo de normativas más robustas como el Reglamento MiCA. Se van a detallar tres casos notorios donde se puede observar la falta de regulación y, por consiguiente, la necesidad de continuar desarrollando normativas que se adecuen a la actualidad.

El colapso de Terra-Luna en mayo de 2022 representó el primer pánico financiero a gran escala en el ecosistema cripto, un crudo recordatorio de la fragilidad sistémica en un entorno sin una red de seguridad regulatoria clara. El evento se centró en la *stablecoin* algorítmica UST, cuyo valor se desplomó en una "espiral de la muerte" que aniquiló miles de millones de dólares en valoración (Liu, Makarov, & Schoar, 2023). Este suceso subraya la pertinencia del Reglamento MiCA, que impone requisitos estrictos de reserva y gobernanza para los emisores de stablecoins, clasificándolos como *Token*s Referenciados a Activos (ARTs) o *Token*s de Dinero Electrónico (EMTs) para evitar precisamente este tipo de inestabilidad (Liu, Makarov, & Schoar, 2023). El caso demostró que la transparencia inherente de la *blockchain*, aunque a menudo es una virtud, puede amplificar los riesgos al acelerar las corridas de capital, reforzando así la necesidad de aplicar el principio de “mismo riesgo, misma regulación” que promueven los organismos internacionales.

Por otro lado, el litigio de la Comisión de Bolsa y Valores de EE. UU. (SEC) contra Ripple Labs se convirtió en un caso fundamental para la delimitación entre los distintos tipos de criptoactivos. La demanda, que acusaba a Ripple de vender el *token* XRP como un valor no registrado, es un ejemplo paradigmático de la inseguridad jurídica generada por la aplicación de leyes de valores tradicionales a una nueva tecnología (Verret, 2025). La sentencia judicial de 2023 diferenció entre las ventas a inversores institucionales, consideradas valores, y las ventas programáticas a minoristas, que no lo eran (Verret, 2025). Esta distinción es crucial y se alinea con la interpretación de autoridades como la CNMV, que ha sostenido que un criptoactivo debe ser considerado un instrumento financiero (*security token*) en función de sus características económicas y no de la tecnología subyacente. Este caso ilustra por qué el Reglamento MiCA excluye de su ámbito a los *security tokens*, ya que estos deben regirse por la normativa de valores ya existente, como MiFID II.

Finalmente, las sanciones impuestas a Binance, el mayor *exchange* de criptomonedas del mundo, evidencian las severas consecuencias de no adherirse a los marcos regulatorios internacionales de prevención de blanqueo de capitales (AML) y conocimiento del cliente (KYC). En 2023, la compañía acordó pagar miles de millones de dólares en multas y su CEO renunció al cargo debido a fallos sistemáticos en el cumplimiento de dichas normativas (Maldonado, 2023). Este caso resalta la importancia de las obligaciones a las que se enfrentan los proveedores de servicios con criptoactivos, como la necesidad en España de inscribirse en el registro del Banco de España con fines de supervisión AML. La lección principal es que, para operar de forma sostenible, las empresas del sector deben priorizar el cumplimiento normativo, un aspecto central en la arquitectura de supervisión que establece MiCA para todos los proveedores de servicios en la Unión Europea.

3. Conclusiones y buenas prácticas extraídas de los casos

El análisis de los casos de tokenización exitosa y de los proyectos que han enfrentado controversias legales y colapsos sistémicos permite extraer una serie de conclusiones y buenas prácticas fundamentales para navegar el ecosistema de la financiación *blockchain*.

Primero, la regulación es inevitable y necesaria para la madurez del sector. El colapso de Terra-Luna no fue solo el fallo de un proyecto, sino la demostración del riesgo sistémico que pueden generar las stablecoins algorítmicas sin un respaldo adecuado. Este suceso,

junto con las sanciones multimillonarias a Binance por deficiencias en sus políticas AML/KYC, ha validado el principio de "mismo riesgo, misma regulación" que impulsan los organismos globales y que se materializa en MiCA. La era de la autorregulación ha terminado; la sostenibilidad a largo plazo exige un cumplimiento normativo riguroso.

Segundo, la sustancia económica prevalece sobre la etiqueta tecnológica. El litigio de la SEC contra Ripple Labs subraya una lección crítica: los reguladores analizarán la función económica de un *token* para determinar si es un valor negociable (*security token*). Denominar a un activo como "*token* de utilidad" no lo exime de la regulación de valores si, en la práctica, se ofrece y percibe como una inversión con expectativa de beneficio. Esto obliga a los emisores a realizar un análisis jurídico profundo y a ser transparentes sobre los derechos que confiere el *token*.

De estos casos se pueden derivan las siguientes buenas prácticas:

- Priorizar el cumplimiento normativo desde el diseño (Compliance by Design): Los proyectos no deben considerar la regulación como un obstáculo a posteriori, sino integrarla desde la fase de diseño del *token* y del modelo de negocio. Esto incluye una clasificación legal clara del activo, la implementación de robustos procedimientos KYC/AML y la preparación para cumplir con los requisitos de transparencia y divulgación de información exigidos por MiCA.

- Transparencia y robustez en el diseño de *token*s: En el caso de los *token*s que aspiran a mantener un valor estable (stablecoins), la transparencia sobre los activos de reserva y los mecanismos de estabilización es innegociable. El caso Terra-Luna demostró que los diseños puramente algorítmicos pueden ser frágiles. Una auditoría externa y una gobernanza clara son esenciales para generar confianza.

- Enfoque en la utilidad real y la creación de valor: Más allá de la especulación, el éxito a largo plazo de un proyecto tokenizado depende de su capacidad para resolver un problema real y crear valor tangible. Plataformas como tZERO o los fondos de Franklin Templeton muestran que la tokenización triunfa cuando mejora procesos existentes, ya sea aumentando la liquidez de activos ilíquidos o haciendo más eficientes las operaciones del mercado.

VII. Conclusiones

1. Principales hallazgos de la investigación

A lo largo de este estudio, se ha realizado un recorrido exhaustivo por el emergente mundo de la financiación basada en tecnología *blockchain*, desde sus cimientos técnicos hasta su compleja realidad regulatoria y práctica. Los principales hallazgos de esta investigación pueden sintetizarse en los siguientes puntos:

En primer lugar, la tecnología *blockchain* ha demostrado ser una fuerza disruptiva en el sector financiero, habilitando un ecosistema alternativo que democratiza el acceso al capital. Modelos como las ICOs, STOs, IEOs e IDOs han permitido a proyectos innovadores financiarse al margen de los canales tradicionales, ofreciendo a su vez nuevas oportunidades de inversión a una audiencia global.

En segundo lugar, el propio mercado ha experimentado una notable evolución. Se ha transitado desde la euforia inicial de las ICOs, caracterizada por la falta de regulación y un alto índice de fraudes, hacia modelos más maduros y seguros como las STOs y las IEOs, que reintroducen elementos de control, ya sea a través del cumplimiento de la normativa de valores o de la diligencia debida realizada por plataformas de intercambio.

En tercer lugar, la respuesta regulatoria, con el Reglamento MiCA como estandarte en Europa, constituye la tendencia más definitoria del sector en la actualidad. Esta nueva normativa busca equilibrar la protección del inversor y la estabilidad financiera con el fomento de la innovación. Al establecer un marco jurídico claro para los criptoactivos y sus proveedores de servicios, MiCA sienta las bases para un mercado más seguro, transparente y legítimo, lo que podría atraer a inversores institucionales y acelerar la adopción masiva.

Finalmente, la aplicación práctica de la tokenización ya está generando beneficios tangibles en las finanzas tradicionales. La capacidad de fraccionar la propiedad, aumentar la liquidez de activos tradicionalmente ilíquidos (como el inmobiliario o el arte) y automatizar procesos complejos (como el pago de dividendos o intereses) mediante contratos inteligentes está optimizando la eficiencia y reduciendo costes operativos.

2. Limitaciones del estudio

A pesar de los esfuerzos por ofrecer un análisis completo y actualizado, este estudio presenta ciertas limitaciones inherentes a la naturaleza del objeto de estudio:

- Dinamismo del sector: El ecosistema *blockchain* y de los criptoactivos evoluciona a una velocidad vertiginosa. Los desarrollos tecnológicos, las nuevas aplicaciones y los cambios en el panorama regulatorio pueden hacer que parte de la información contenida en este trabajo quede desactualizada en un corto período. El estudio representa una fotografía del estado del arte a fecha de 2025.
- Impacto incipiente de la regulación: Dado que la plena aplicación del Reglamento MiCA es reciente, su impacto real y a largo plazo en el mercado europeo de criptoactivos aún no ha podido ser medido empíricamente. Las conclusiones sobre sus efectos se basan en proyecciones y análisis de su contenido, no en datos históricos consolidados.
- Fuentes de información: La investigación se basa exclusivamente en fuentes secundarias de acceso público. No se han realizado entrevistas con desarrolladores de proyectos, reguladores o inversores, lo que podría haber aportado perspectivas más profundas y matizadas sobre ciertos aspectos del ecosistema.
- Profundidad técnica: Si bien se explican los conceptos técnicos necesarios para la comprensión del tema, el trabajo no profundiza en los aspectos más complejos de la criptografía o la programación de contratos inteligentes, ya que su enfoque principal es económico y jurídico.

3. Propuestas de investigación o desarrollo futuro

El carácter dinámico y la creciente relevancia de la financiación *blockchain* abren numerosas vías para futuras investigaciones. A continuación, se proponen algunas líneas de trabajo:

Una de las áreas más relevantes es el análisis empírico del impacto del reglamento MiCA. Sería muy valioso realizar un estudio cuantitativo para evaluar el efecto económico de esta normativa en el mercado de criptoactivos de la Unión Europea después de su implementación completa. Una investigación de este tipo podría analizar métricas clave

como el volumen de *token*s emitidos, el nivel de inversión en nuevas empresas del sector, y cómo han evolucionado los precios y la volatilidad.

Otra línea de investigación prometedora es un estudio comparativo de marcos regulatorios. Una investigación exhaustiva que compare la regulación en la Unión Europea (MiCA), el enfoque fragmentado de Estados Unidos y los marcos de mercados asiáticos como Singapur o Hong Kong podría identificar las mejores prácticas a nivel global. Este análisis sería crucial para comprender los desafíos de una posible armonización regulatoria en el futuro.

Además, la regulación de las Finanzas Descentralizadas (DeFi) representa un desafío único. Dado que MiCA se enfoca principalmente en entidades centralizadas, una investigación futura podría explorar las complejidades técnicas y legales de aplicar un marco normativo a protocolos DeFi que son inherentemente descentralizados y autónomos. Esta línea de estudio podría proponer soluciones innovadoras para cerrar esta brecha regulatoria.

Finalmente, la tokenización de Activos del Mundo Real (RWA) en España ofrece una oportunidad de investigación específica. Sería muy útil realizar un estudio que se centre en los retos y oportunidades de tokenizar activos tangibles (como propiedades inmobiliarias o productos agrícolas) dentro del marco legal español. Este análisis podría examinar cómo MiCA interactúa con la legislación nacional en áreas como la propiedad, los registros públicos y el derecho mercantil.

ANEXO I. Relación con los ODS

Este trabajo de investigación sobre las nuevas fórmulas de financiación mediante tecnología *blockchain* se relaciona de manera directa con el Objetivo de Desarrollo Sostenible 9: Industria, Innovación e Infraestructura (ONU, s.f.) .

El ODS 9 busca construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación. Dentro de este objetivo, la meta 9.3 es especialmente pertinente: "Aumentar el acceso de las pequeñas industrias y otras empresas, particularmente en los países en desarrollo, a los servicios financieros, incluidos créditos asequibles, y su integración en las cadenas de valor y los mercados" (ONU, s.f.).

La tecnología *blockchain* y la tokenización, como se ha descrito a lo largo de este documento, contribuyen a esta meta de varias maneras:

1. Fomento de la innovación: La propia *blockchain* es una infraestructura tecnológica innovadora que permite el desarrollo de nuevas aplicaciones y modelos de negocio. La financiación a través de *token*s es una innovación radical en el campo de las finanzas corporativas.

2. Acceso a servicios financieros: Los modelos de financiación descentralizada reducen las barreras geográficas y la dependencia de intermediarios financieros tradicionales. Esto permite que startups y pymes de cualquier parte del mundo puedan presentar sus proyectos a una base de inversores global, obteniendo el capital necesario para crecer y generar empleo, alineándose directamente con la meta 9.3.

3. Inclusión financiera para inversores: La propiedad fraccionada que permite la tokenización hace posible que pequeños inversores puedan participar en proyectos y activos que antes les eran inaccesibles, democratizando la inversión y promoviendo un ecosistema financiero más inclusivo.

4. Desarrollo de nuevas infraestructuras de mercado: La creación de mercados secundarios para activos tokenizados representa la construcción de una nueva infraestructura financiera más eficiente, transparente y operativa 24/7, lo que moderniza y fortalece el tejido industrial.

El desarrollo de un marco regulatorio sólido como MiCA es fundamental para que esta contribución sea sostenible, garantizando que la innovación se desarrolle dentro de un entorno seguro que proteja a los inversores y preserve la estabilidad financiera, condiciones indispensables para un crecimiento económico sostenido.

ANEXO II. Bibliografía

Adachi, Mitsu. (2022). Stablecoins' role in crypto and beyond: functions, risks and policy. *Macroprudential Bulletin 18*.

Ahn, J., Yi, E., & Kim, M. (2024). Blockchain Consensus Mechanisms: A Bibliometric Analysis (2014–2024) Using VOSviewer and R Bibliometrix. *MDPI*. doi:https://doi.org/10.3390/info15100644

Aldasoro, I., Cornelli, G., Frost, J., Wilkens Koo, P., Lewrick, U., & Shreeti, V. (2025). *Tokenisation of government bonds: assesments and roadmap.* BIS.

Antonopoulos, A. M. (2019). *Mastering Ethereum : building smart contracts and DApps.* Sebastopol.

Asmare, D., Legese, F., & Birara, J. (2023). Blockchain Technology: Understanding its Meaning, Architecture, and Diverse Applications. *ResearchGate*.

Banisadr, E. (1 de Febrero de 2018). *How $800k Evaporated from the PoWH Coin Ponzi Scheme Overnight*. Obtenido de Medium: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://medium.com/%40ebanisadr/how-800k-evaporated-from-the-powh-coin-ponzi-scheme-overnight-1b025c33b530&ved=2ahUKEwjW6ebciq6PAxW2_rsIHZ7gLvwQFnoECB8QAQ&usg=AOvVaw16AxLi92MG26iDZF74h-_D

Banoo Muradi, S., & Kia Chim, Y. (2022). Identification of selection criteria for blockchain platforms. *IEEE*.

Beeple. (11 de marzo de 2021). *Everydays: The First 5000 Days*. Obtenido de Christie's: https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924

Buterin, V. (2014). A Next Generation Smart Contract & Decentralized Application Platform. *Ethereum*.

Che, J., Xia, X., & Lo, D. (2021). Maintenance-Related Concerns for Post-deployed. *Monash University*.

CNMV. (s.f.). *MiCA: Nueva regulación de criptoactivos*. Obtenido de CNMV: https://www.cnmv.es/Portal/mica/regulacion-criptoactivos?lang=es#:~:text=La%20CNMV%20es%20la%20autoridad,Banco%20de%20Espa%C3%B1a

ESMA. (2024). *Consultation Paper on the draft Guidelines on the conditions and criteria of qualification of crypto-assets as financial instruments.* ESMA.

España, B. d. (9 de Febrero de 2021). *CNMV.* Obtenido de Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión: https://www.cnmv.es/portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D#:~:text=para%20la%20emisi%C3%B3n%20de%20criptoactivos,u%20otras%20autoridades%20p%C3%BAblicas%20y

Fabus, J., Kremenova, I., Stalmasekova, N., & Kvasnicova-Galovicova, T. (2024). An Empirical Examination of Bitcoin's Halving Effects: Assessing Cryptocurrency Sustainability within the Landscape of Financial Technologies. *Journal of Risk and Financial Management*.

finReg360. (23 de 07 de 2024). *La CNMV da a conocer los modelos para solicitar las licencias requeridas por el reglamento MiCA*. Obtenido de finReg360 - Firma de regulación financiera: https://finreg360.com/alerta/la-cnmv-da-a-conocer-los-modelos-para-solicitar-las-licencias-requeridas-por-el-reglamento-mica/#:~:text=Los%20actuales%20proveedores%20que%20ya,de%20la%20licencia%20lo%20antes

FinReg360. (30 de 12 de 2024). *La CNMV deroga la circular sobre publicidad de criptoactivos ante la próxima aplicación del reglamento MiCA*. Obtenido de finReg360.com: https://finreg360.com/alerta/la-cnmv-deroga-la-circular-sobre-publicidad-sobre-criptoactivos-ante-la-proxima-fecha-de-aplicacion-de-mica/#:~:text=El%20reglamento%20MiCA%2C,miembros%20y%2C%20por%20primera%20vez

Furnari, S. L. (2021). Trough Equity Crowdfunding Evolution and Involution: Initial Coin Offering and Initial Exchange Offer. *КИБЕРПРОСТРАНСТВО*.

Garcia-Fuentes, G. (5 de Junio de 2024). *La CNMV resuelve dudas sobre criptoactivos en un documento de preguntas y respuestas*. Obtenido de Garrigues: https://www.garrigues.com/es_ES/noticia/cnmv-resuelve-dudas-criptoactivos-documento-preguntas-respuestas#:~:text=1,destacar%20la%20ya%20existencia%20del

Google Finance. (20 de Abril de 2024). *Google Finance*.

Gopan, A. (2023). Ethereum Network. *IJNRD*.

Group, W. B. (Noviembre de 2024). *Security Token Offerings.* World Bank Group.

Hedera. (28 de Agosto de 2025). *Testing Smart Contracts*. Obtenido de Hedera: https://hedera.com/learning/smart-contracts/testing-smart-contracts

How to time-stamp a digital document. (1991). En S. Haber, & W. S. Scornetta, *Volume 26, Number 4* (págs. 99-111). Journal of Cyptology.

HSBC. (27 de Marzo de 2024). *HSBC Gold Token*. Obtenido de HSBC: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.hsbc.com.hk/content/dam/hsbc/hk/docs/investments/gold-token/principal-brochure.pdf&ved=2ahUKEwi46M3HqraPAxUhm_0HHV5WPPMQFnoECBkQAQ&usg=AOvVaw2fiTpZmgfh6ia_-G2p99kS

Huang, Y., & Wang, B. (2021). Research and Application of Smart Contract Based on Ethereum Blockchain. *Journal of Physics Conference Series*.

IT Faculty. (2018). History of Blockchain. *ICAEW*.

Jezek, K. (2020). Ethereum Data Structure. *University of Sydney*.

Katiyar, N., Verma, S., Kumar, M., Kumar, P., & Sahu, D. (2023). Decentralized Consensus Mechanisms in Blockchain: A Comparative Analysis. *IJRITCC*.

Kobusinska, A., & Wilczynski, G. (2022). Blocked-based Solidity — a Service for Graphically Creating the Smart Contracts in Solidity Programming Language. *55th Hawaii International Conference on System Sciences.* Oahu.

Kumar Sharma, T. (18 de enero de 2025). *Security Tokens vs Utility Tokens*. Obtenido de Blockchain Council: https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-guide/

Kumar, S. (2020). *Bitcoin and blockchain : history and current applications.* Boca Raton: CRC Press, Taylor & Francis Group.

Laurent, P., Chollet, T., Burke, M., & Seers, T. (2019). *The tokenization of assets is disrupting the financial industry. Are you ready?* Deloitte.

Liu, J., Makarov, I., & Schoar, A. (Abril de 2023). Anatomy of a Run: The Terra Luna Crash. *NBER*. doi:10.3386/w31160

Magnusson, S., & Renhage, D. (2022). Initial Exchange Offerings (IEOs) and Initial DEX Offerings (IDOs). *CBS*.

Maldonado, J. (22 de Noviembre de 2023). *Binance y la lección aprendida sobre seguir las regulaciones*. Obtenido de bit2me: https://news.bit2me.com/binance-leccion-aprendida-seguir-las-regulaciones

Mansa, J., & Rosenton, M. (22 de abril de 2024). *What Are Crypto Tokens, and How Do They Work?* Obtenido de Investopedia: https://www.investopedia.com/terms/c/crypto-token.asp

Marin, O., Cioara, T., Toderean, L., Mitrea, D., & Anghel, I. (09 de noviembre de 2023). Review of Blockchain Tokens Creation and Valuation. *MDPI*, 15. doi:https://doi.org/10.3390/fi15120382

Martinez, A., & Gonzalez, R. (2024). A technical history of blockchain design, innovation, and narratives: Part I. *Foundation Capital*.

Melashych, S. (22 de mayo de 2025). *The Pros and Cons of STO: What Businesses Need to Know*. Obtenido de Agilie: https://agilie.com/blog/the-pros-and-cons-of-sto

Metamask. (28 de Agosto de 2025). *MetaMask*. Obtenido de How to estimate the gas fee: https://support.metamask.io/more-web3/learn/how-to-estimate-the-gas-fee/

MiCA, R. (2023). Reglamento MiCA. *Diario Oficial de la UE*. Obtenido de https://eur-lex.europa.eu/ES/legal-content/summary/european-crypto-assets-regulation-

mica.html#:~:text=El%20Reglamento%20%20,proveedores%20de%20servicios%20de%20criptoactivos

Moncloa, L. (26 de 10 de 2023). *España adelanta la aplicación del primer Reglamento del mundo sobre el mercado de criptoactivos*. Obtenido de La Moncloa: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/paginas/2023/261023-reglamento-europeo-mercado-criptoactivos.aspx#:~:text=servicios%20de%20inversi%C3%B3n%20de%20MiFID%2C,ser%20autorizados%20por%20la%20CNMV

NadlabAdmin. (3 de Junio de 2025). *7 Easy Tips to Reduce Gas Optimization in Smart Contracts*. Obtenido de NadCab Labs: https://www.nadcab.com/blog/gas-optimization-in-smart-contracts

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org*.

ONU. (s.f.). *ODS 9*. Obtenido de Objetivos de Desarrollo Sostenible: https://www.un.org/sustainabledevelopment/es/infrastructure/

Pereira, É., Ferreira, P., & Quintino, D. (2022). Non-Fungible Tokens (NFTs) and Cryptocurrencies: Efficiency and Comovements. *FinTech*. doi:https://doi.org/10.3390/fintech1040023

Polcumpally, A., Kumar, K., Kumar, A., & Samadhiya, A. (2024). Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions. *Heliyon*.

QuillAuditsAdmin. (30 de Junio de 2025). *Smart Contract Vulnerabilities, Risks and How to mitigate them*. Obtenido de QuillAudits: https://www.quillaudits.com/blog/smart-contract/smart-contract-vulnerabilities

Qunie. (2024). The Evolution of Tokenization in the Financial Sector and the Feasibility of the use of Blockchain Technology for RegTech/SupTech. *JFSA*.

Rahardja, U., Hidayanto, A. N., Lutfiani, N., Febiani, D. A., & Aini, Q. (2021). Immutability of Distributed Hash Model on Blockchain Node Storage. *Scientific Journal of Informatics*, Vol.8, No.1.

Rasul, H. (2018). Does Bitcoin need regulation? An analysis of Bitcoin's Decentralized Nature as a Security and Regulatory Concern for Governments. *Seton Hall University*.

Release, P. (17 de Julio de 2023). *FSB finalises global regulatory framework for crypto-asset activities*. Obtenido de Financial Stability Board: https://www.fsb.org/2023/07/fsb-finalises-global-regulatory-framework-for-crypto-asset-activities/#:~:text=The%20framework%20consists%20of%20two,distinct%20sets%20of%20recommendations

Roopika, J. (2020). Blockchain Technology: History, Concepts, and Applications. *International Research Journal of Engineering and Technology (IRJET)*.

Sánchez, E. (21 de agosto de 2023). *¿Cómo funciona Reental?* Obtenido de Reental: https://www.reental.co/blog/como-funciona-reental

Šapkauskienė, A., & Višinskaitė, I. (2020). INITIAL COIN OFFERINGS (ICOs): BENEFITS, RISKS AND SUCCESS MEASURES. *JSSDOI*.

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations. *IEEE*, 2-3.

Shi, J. (2024). The Evolution and Future of Cryptocurrency-Based Fundraising Mechanisms. *JBBA*.

Shine, I. (8 de Mayo de 2024). *La normativa sobre criptomonedas está cambiando en todo el mundo. Esto es lo que hay que saber*. Obtenido de World Economic Forum: https://es.weforum.org/stories/2024/05/la-normativa-sobre-criptomonedas-esta-cambiando-en-todo-el-mundo-esto-es-lo-que-necesitas-saber/#:~:text=criptomonedas

Solmonte, S. (2023). An Analyisis of the Ethereum Proof of Stake Protocol. *Universitá di Bologna*.

Soni, U., Fines, O., & Sun, J. (2025). An Investment Perspective on Tokenization — Part I . *CFA Institute - Research & Policy Center*.

Staff, C. (26 de Febrero de 2025). *What was the DAO?* Obtenido de Gemini.com: https://www.gemini.com/cryptopedia/the-dao-hack-

makerdao?_gl=1*as2aid*_ga*NTA4NjY3NDkuMTc0MzQ5NjE3MQ..*_ga_WC57KJ50ZZ*MTc0NTQ4MzM3Ny4yNi4xLjE3NDU0ODQ4NTUuMC4wLjA.

Stein, M. (25 de Agosto de 2025). *Surge*. Obtenido de Ethereum Gas Explained: A Guide to Gas Fees: https://www.surgewomen.io/learn-about-web3/ethereum-gas-explained-a-guide-to-gas-fees

Verret, J. (20 de Agosto de 2025). *This is Finally the End: The Ripple Case Concludes as Predicte*. Obtenido de National Law Review: https://natlawreview.com/article/finally-end-ripple-case-concludes-predicted

Victor, F., & Lüders, B. (2018). Measuring Ethereum-based ERC-20 Networks. *Technische Universität Berlin*.

Vikas, N., & Satpalsing , D. (2020). Analysis of Blockchain Algorithms. *IJIRSET*, Vol. 9, No. 3.

Wandmacher, R. (2019). *Tokenomics.* Paris: Springer.

Wilson, M. (22 de Abril de 2025). *Mainnet vs. Testnet*. Obtenido de Blockchain Council: https://www.blockchain-council.org/blockchain/mainnet-vs-testnet/

Wood, G. (2014). Ethereum: A secure decentralisez generalized transaction ledger. *Github.com*.

Wu, T. C., & Ho, C. B. (2023). Blockchain Revolutionizing in Emergency Medicine: A Scoping Review of Patient Journey through the ED. *National Library of Medicine*, 2-3. doi:https://doi.org/10.3390/healthcare11182497

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. *National Institute of Standards and Technology*.

Zamani, E. (2022). The Bitcoin protocol as a system of power. Ethics and Information Technology. *University of Sheffield*.