UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas

# UNIVERSITAT POLITÈCNICA DE VALÈNCIA

## Facultad de Administración y Dirección de Empresas

# ESTUDIO DE LA PROBLEMÁTICA EN LA INVERSIÓN EN CRIPTOMONEDAS

Trabajo Fin de Grado

Grado en Administración y Dirección de Empresas

AUTOR/A: Donet Pellicer, Maria

Tutor/a: Moya Clemente, Ismael

CURSO ACADÉMICO: 2023/2024

## AGRADECIMIENTOS

A mis amigos y mi familia,
por su apoyo, cariño
y confianza incondicional.

A mi tutor, Ismael Moya,
por la atención,
resolución de dudas, problemas
y por haber sido un gran profesor.

A la Universidad Politécnica de Valencia,
por la calidad en su formación,
docentes y oportunidades.

## ÍNDICE DE FIGURAS

# ÍNDICE DE CONTENIDO

# ESTUDIO DE LA PROBLEMÁTICA EN LA INVERSIÓN EN CRIPTOMONEDAS

AUTOR/A: MARÍA DONET PELLICER

## RESUMEN

En este trabajo de final de grado se pretende realizar un estudio, principalmente, sobre las criptomonedas, y un análisis de la posible burbuja inversora que les ha afectado.

Para ello, se introducirán estos tipos de monedas, su legalidad, futuro y expectativas; explicando, fundamentalmente, qué son estas monedas digitales, en qué consiste el procedimiento de inversión y negociación, los principales tipos de moneda virtual (Bitcoin y Ethereum), cuál es la problemática actual que está ocurriendo con plataformas de exchange, como por ejemplo, la crisis y caída en bancarrota de algunas plataformas como FTX, cuyo fundador está siendo juzgado por presunta estafa, con posibilidad de causar un efecto contagio o la congelación de cuentas ("corralito") efectuado por Celsius, destacada entidad de préstamo en el ámbito de las monedas digitales y figura prominente dentro del sector de las finanzas descentralizadas que ha sido el detonante de una reciente caída en los valores de Bitcoin y Ethereum.

Debido a las medidas de recuperación económica durante la pandemia, en el que los bancos centrales han seguido con medidas de apoyo como los bajos tipos de interés, el sector tecnológico fue uno de los grandes beneficiados. Sin embargo, las subidas en los tipos de interés han provocado que numerosos inversores hayan dejado a un lado los activos de mayor riesgo para pivotar hacia aquellos más seguros como la renta fija.

En este contexto, en el 2022, las 20 divisas digitales con mayor capitalización de mercado han perdido de media más del 50% de su cotización.

Por otra parte, se analizarán los aspectos de estas criptomonedas que puedan ser indicativos de una posible burbuja inversora relacionándolos con otros casos destacados de burbujas financieras.

Por lo tanto, la finalidad de este trabajo es clarificar qué son las criptomonedas dado que se trata de un mercado que negocia un gran volumen de fondos en la actualidad y que a su vez es desconocido por una buena parte de los inversores que en él intervienen y que puede estar muy relacionado con otras burbujas financieras que han sucedido.

## RESUM

En aquest treball de final de grau es pretén fer un estudi, principalment, sobre les criptomonedes, i un anàlisi de la possible bombolla inversora que els ha afectat.

Per això, s'introduiran aquests tipus de monedes, la seua legalitat, futur i expectatives; explicant, fonamentalment, què són aquestes monedes digitals, en què consisteix el procediment d'inversió i negociació, els principals tipus de moneda virtual (Bitcoin i Ethereum), quina és la problemàtica actual que està passant amb plataformes d'exchange, com ara la crisi i caiguda en fallida d'algunes plataformes com FTX, el fundador el qual está siguent jutjat per presumpta estafa, amb possibilitat de causar un efecte contagi o la congelació de comptes efectuat per Celsius, destacada entitat de prèstec en l'àmbit de les monedes digitals i figura prominent dins del sector de les finances descentralitzades que ha sigut el detonant d'una caiguda recent en els valors de Bitcoin i Ethereum.

A causa de les mesures de recuperació econòmica durant la pandèmia, en què els bancs centrals han seguit amb mesures de suport com els tipus d'interès baixos, el sector tecnològic va ser un dels grans beneficiats. Tot i això, les pujades en els tipus d'interès han provocat que nombrosos inversors hagin deixat de banda els actius de més risc per pivotar cap a aquells més segurs com la renda fixa.

En aquest context, el 2022, les 20 divises digitals amb més capitalització de mercat han perdut de mitjana més del 50% de la cotització.

D'altra banda, s'analitzaran els aspectes d'aquestes criptomonedes que puguen ser indicatius d'una possible bombolla inversora relacionant-los amb altres casos destacats de bombolles financeres.

Per tant, la finalitat d'aquest treball és clarificar què són les criptomonedes donat que es tracta d'un mercat que negocia un gran volum de fons actualment i que alhora és desconegut per una bona part dels inversors que hi intervenen i que pot estar molt relacionat amb altres bombolles financeres que han passat.

## ABSTRACT

In this final degree thesis we intend to carry out a study, mainly, on cryptocurrencies, and an analysis of the possible investment bubble that has affected them.

For this purpose, we will introduce these types of currencies, their legality, future and expectations; explaining, fundamentally, what are these digital currencies, what is the procedure of investment and negotiation, the main types of virtual currency (Bitcoin and Ethereum), what is the current problem that is happening with exchange platforms, such as the crisis and bankruptcy of some platforms such as FTX, whose founder is on trial for alleged fraud, with the possibility of causing a contagion effect or the freezing of accounts carried out by Celsius, leading digital currency lender and prominent figure within decentralized finance sector which has been the trigger for a recent drop in Bitcoin and Ethereum values.

Due to the economic recovery measures during the pandemic, in which central banks have continued with supportive measures such as low interest rates, the technology sector was one of the big beneficiaries. However, rising interest rates have caused many investors to shift away from riskier assets and into safer assets such as fixed income.

In this context, in 2022, the 20 digital currencies with the largest market capitalization have lost on average more than 50% of their price.

On the other hand, the aspects of these cryptocurrencies that may be indicative of a possible investment bubble will be analyzed by relating them to other prominent cases of financial bubbles.

Therefore, the purpose of this work is to clarify what cryptocurrencies are, given that this is a market that currently trades a large volume of funds and which is unknown to a large part of the investors involved in it, and which may be closely related to other financial bubbles that have occurred.

# 1. INTRODUCCIÓN

## 1.1. Contexto y justificación

La inversión en criptomonedas ha experimentado un crecimiento significativo en los últimos años, atrayendo la atención de inversores y particulares de todo el mundo. Estas monedas digitales descentralizadas ofrecen características únicas, como la seguridad, la privacidad y la eliminación de intermediarios, lo que ha generado un gran interés en su potencial de inversión. No obstante, también surgen desafíos y problemáticas relacionadas con la inversión en criptomonedas lo cual será nuestro objeto de estudio, con el objetivo de comprender mejor los riesgos y desafíos que enfrentan los inversores en esta forma de inversión.

El primer aspecto que considerar es la volatilidad de las criptomonedas. A diferencia de las monedas tradicionales, el valor de las criptomonedas puede experimentar fluctuaciones extremas en periodos de tiempo muy cortos. Esta volatilidad puede ser atractiva para algunos inversores que buscan obtener ganancias rápidas, pero también puede generar pérdidas significativas y dificultar la toma de decisiones de inversión informadas.

Otro desafío importante es la seguridad. Aunque las criptomonedas ofrecen un alto nivel de seguridad mediante tecnologías criptográficas, también están expuestas a riesgos como hackeos, robos y estafas. La falta de regulación en muchos países y la ausencia de un respaldo gubernamental hacen que los inversores sean más vulnerables a posibles ataques cibernéticos y pérdida de fondos.

La falta de información y educación adecuada implica otro obstáculo para los inversores en criptomonedas, debido que muchas personas carecen de los conocimientos necesarios para tomar decisiones de inversión fundamentadas y para trabajar con este tipo de tecnología tan compleja. La falta de transparencia y la presencia de esquemas fraudulentos dificultan aún más la identificación de oportunidades legítimas.

En este trabajo, se analizarán también las implicaciones legales y regulatorias de la inversión en criptomonedas. Dado que éstas operan en un entorno global y transfronterizo, surgen desafíos en términos de jurisdicción, impuestos y cumplimiento normativo. Se explorarán las diferentes regulaciones existentes en varios países y se evaluará su impacto en la inversión en criptomonedas.

## 1.2. Objetivos

Los objetivos específicos de este trabajo de final de grado se centran en analizar la economía de las criptomonedas, para comprender cómo estos factores contribuyen a su valor y su aceptación en el mercado global; examinar los tipos de criptomonedas más influyentes, específicamente Bitcoin y Ethereum, identificando sus características distintivas, sus tecnologías subyacentes y su papel en el ecosistema de las criptomonedas para establecer una base de comparación y comprensión de la diversidad existente en este campo. También, explorar los aspectos legales y regulatorios que afectan al mercado de las criptomonedas, incluyendo las variaciones entre jurisdicciones y los desafíos que plantean para los reguladores, con el objetivo de identificar las tendencias actuales y futuras en la regulación de estas divisas digitales. Por otro lado, investigar los riesgos y desafíos asociados, incluyendo la volatilidad del mercado, los riesgos de seguridad y los problemas éticos, para proporcionar una evaluación crítica de los obstáculos que deben superarse para una adopción más amplia. Asimismo, analizar la problemática específica de las plataformas exchange, evaluando los riesgos de seguridad, las cuestiones de regulación y la importancia de estas plataformas para el funcionamiento del mercado de criptomonedas, con el fin de entender los desafíos operativos y regulatorios; evaluar la situación actual del mercado de criptomonedas, observando las tendencias de mercado, la adopción por parte de inversores y consumidores, y la respuesta institucional, para ofrecer una visión completa del estado actual y las perspectivas de futuro y, finalmente, realizar una comparativa con burbujas financieras históricas para identificar similitudes y diferencias con el fenómeno de las criptomonedas, con el objetivo de extraer lecciones aprendidas y aplicarlas al contexto actual.

Con estos objetivos se busca proporcionar una comprensión holística y detallada de las criptomonedas, sus desafíos, oportunidades y su posición dentro del panorama financiero global, contribuyendo así al cuerpo de conocimiento sobre este tema emergente y de creciente importancia.

## 1.3. Metodología

Para la realización de este trabajo, se ha consultado y analizado el material siguiente:

- Libros referentes a las criptomonedas, su sistema y la blockchain; así como sus medios de adquisición, utilidades e información, fundamentalmente, acerca de los dos principales criptoactivos comentados, Bitcoin y Ethereum.

- Blogs, foros y páginas web de Internet especializados en los activos estudiados.

- Trabajos de final de grado, máster y tesis doctorales que comparten el objeto de análisis o cuyo trabajo es referente a alguna de las secciones específicas de este estudio.

- Informes académicos realizados por expertos en la materia o por instituciones como el Banco de España.

- Periódicos, en formato digital, que han sido utilizados para conocer los hechos que han ido sucediendo durante la elaboración del trabajo.

# 2. MARCO TEÓRICO

El marco conceptual que subyace a los criptoactivos es extenso, involucrando diversas disciplinas que incluyen economía, tecnología, ciberseguridad y normativas. Un sistema de criptomonedas está compuesto por la red de pares (P2P), la tecnología de cadena de bloques (blockchain), el protocolo de transacciones y los procedimientos para la creación de nuevas unidades monetarias.

La estructura de **red peer-to-peer (P2P)** implica que las estaciones de trabajo funcionan como clientes y servidores, facilitando así un modelo de intercambio de servicios de manera simultánea. Este tipo de red se caracteriza por su naturaleza descentralizada y su accesibilidad pública, eliminando la necesidad de una entidad central o de una jerarquía definida dentro del sistema. Cada participante o nodo es independiente, determinando su propio grado de contribución al conjunto de la red. Uno de los desafíos más significativos reside en asegurar la coherencia y la replicación de la información a través de todos los nodos, lo cual garantiza la propagación efectiva de las transacciones y las actualizaciones dentro de la cadena de bloques (Antonopoulos, A. M. 2014).

Respecto la **tecnología blockchain**, ésta se compone de tres partes combinadas e integradas a través de las cuales se cumple un propósito determinado: actuar como un libro de contabilidad digital descentralizado y seguro para registrar y validar todas las transacciones relacionadas con la criptomoneda.

1. La criptografía: El término criptomoneda se refiere a un medio de intercambio digital o virtual, el cual se encuentra protegido por técnicas de cifrado avanzadas que previenen su falsificación o duplicación (Décourt, Chohan & Perugini, 2017). Una de las propiedades distintivas de los criptoactivos es su naturaleza descentralizada, lo cual significa que no están sujetas a la supervisión o control de ninguna entidad central o gubernamental, permitiendo así que las transacciones se realicen sin la intervención de bancos o entidades financieras, evadiendo de esta manera las comisiones que dichas instituciones podrían aplicar. Asimismo, las divisas digitales no pueden ser convertidas directamente en monedas de curso legal emitidas por el gobierno ni pueden ser intercambiadas por bienes de valor intrínseco como serían las monedas de oro o plata.

    - Funciones hash: Se refieren a fórmulas matemáticas complejas que reciben una entrada, conocida como "mensaje", y producen como resultado una secuencia de caracteres de tamaño constante. Estas fórmulas son esenciales dentro del campo de la criptografía puesto que desempeñan un papel crucial en la preservación de la integridad y la verificación de la autenticidad de los datos. La principal función de una función hash es generar un resumen (hash) de un determinado conjunto de datos.

La correspondencia entre los valores hash sugiere que los datos originales permanecen sin alteraciones, ya que cualquier modificación, incluso mínima, en el contenido de los datos originará un valor hash distinto, facilitando así la detección de manipulaciones o corrupciones. Las funciones hash pueden utilizarse para generar claves criptográficas a partir de datos aleatorios. En la criptografía moderna, las funciones hash seguras, como SHA-256 y SHA-3, se utilizan como componentes clave en algoritmos criptográficos.

Respecto las *blockchains*, estas utilizan funciones hash para enlazar bloques y garantizar la integridad de la cadena. Cada bloque contiene el hash del bloque anterior, lo cual crea una estructura inmutable. Además, las criptomonedas utilizan funciones hash para generar direcciones de billetera y validar transacciones.

Cabe destacar que la elección de una función hash segura y apropiada es crucial en criptografía puesto que las funciones hash inseguras o vulnerables pueden comprometer la seguridad de las aplicaciones y los sistemas.

2. El consenso: Este constituye un elemento fundamental para los participantes de la blockchain. Dicho consenso se apoya en un protocolo unificado que verifica y ratifica las transacciones efectuadas, garantizando su carácter irreversible. Asimismo, debe ser imperativo que este mecanismo de consenso ofrezca a todos los participantes una versión inalterable y actualizada del registro de transacciones ejecutadas en la blockchain (Preukschat, A. 2017).

3. La tecnología de cadena de bloques, o blockchain, constituye un tipo de base de datos distribuida que confiere a cada criptomoneda un carácter único debido a que cada operación financiera se registra en un "libro" digital denominado blockchain. Esta tecnología se fundamenta en principios de criptografía de clave pública y privada, lo que asegura la confidencialidad de las transacciones. En esencia, funciona como un monedero digital donde se gestionan las criptomonedas y se documentan las operaciones efectuadas. Los responsables de validar y registrar estas transacciones en la blockchain son los mineros, quienes reciben como compensación las comisiones pagadas por los usuarios al efectuar transacciones y aportan su capacidad de procesamiento computacional con el objetivo de verificar las transacciones y, consecuentemente, obtener criptomonedas como recompensa. Este proceso, conocido como minería, implica la resolución de complejos problemas matemáticos (Vásquez-Leiva, 2014).

   Para que una transacción sea incorporada a la blockchain, todas las operaciones deben adherirse a un conjunto uniforme de reglas o protocolo, lo cual valida el bloque en cuestión y la información contenida en él. Tras completar este procedimiento, la cadena procede a generar el siguiente bloque, manteniendo la información previamente registrada segura e inmodificable mediante el uso de técnicas criptográficas.

La blockchain se compone de los siguientes elementos básicos:

- Los nodos, los cuales deben operar bajo un software o protocolo uniforme para facilitar la intercomunicación. En el contexto de una blockchain pública, no se requiere que los nodos revelen su identidad para participar, a diferencia de una blockchain privada, donde los nodos se identifican mutuamente y pueden tener características homogéneas.

- La red P2P, abordada anteriormente.

- Un protocolo uniforme implementado como software, que establece un sistema de comunicación estandarizado entre los ordenadores (nodos) que forman parte de la red, con la finalidad de validar y conservar de manera coherente la información registrada dentro de una red de pares (P2P).

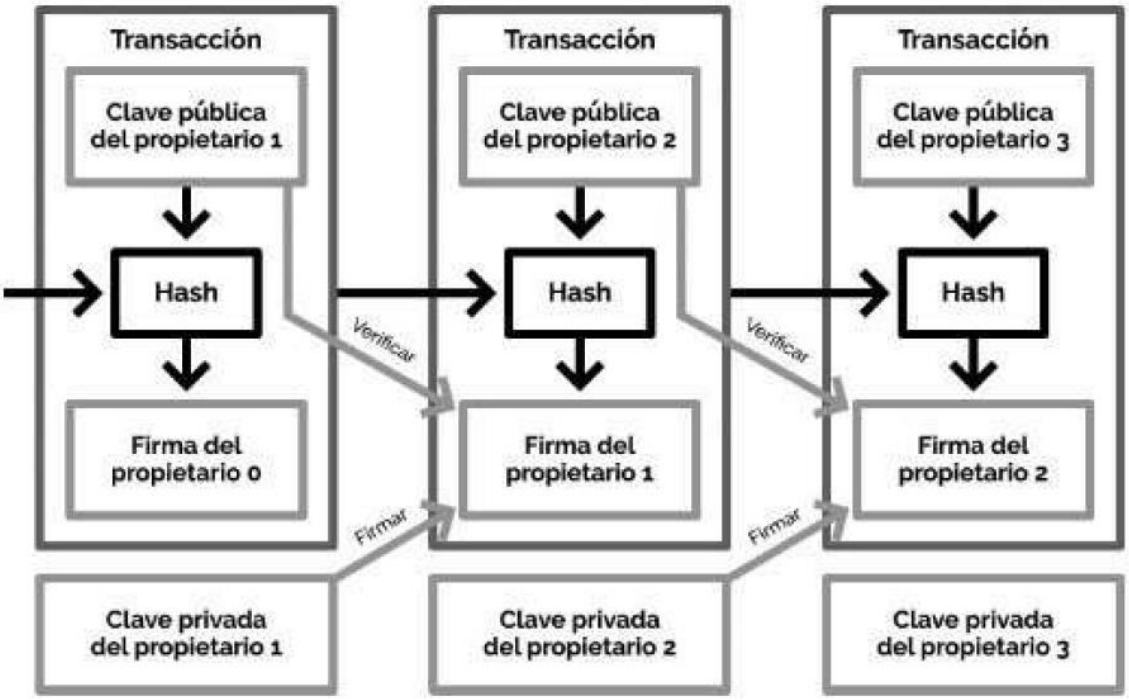
- Un sistema descentralizado en el cual los ordenadores interconectados ejercen control sobre la red, puesto que no prevalece una estructura jerárquica entre los nodos, particularmente en el caso de una blockchain pública.

Un aspecto crítico a considerar es el consumo de energía requerido para sostener la blockchain y asegurar la red. Los mineros y los nodos son incentivados para preservar la funcionalidad de esta mediante una recompensa establecida que se otorga cada diez bloques, la cual experimenta un ajuste cada cuatro años; de este modo, se les compensa por el gasto energético, el esfuerzo computacional y el tiempo invertido en dichas operaciones. No obstante, en el escenario de que la compensación por este esfuerzo cese o deje de ser económicamente viable, existe el riesgo de que los mineros y nodos abandonen sus labores en la validación de transacciones y en el mantenimiento de la estabilidad de la red.

Siguiendo con la composición de un sistema de criptomonedas, el **método transaccional** se fundamenta en el empleo de claves derivadas de técnicas de criptografía asimétrica. Las claves públicas, que son de conocimiento general, actúan como direcciones para el envío o recepción de activos digitales. Estas se componen de entradas (inputs), que son outputs de transacciones previas, uniendo todos los balances en criptomonedas en una o varias salidas nuevas. Dichas entradas son agrupadas dentro de bloques y son accesibles para quienes dispongan de acceso a la blockchain. Los balances contenidos en los inputs seleccionados se utilizan en su totalidad de tal manera que, si el total de los balances en los outputs es menor al de los inputs, la diferencia se destina como comisión (Preukschat, A. 2017) para los mineros. Estos últimos adjuntan en un documento el número total de transacciones pendientes de verificación, junto al último bloque confirmado en la cadena de bloques conocida. Seguidamente, un minero debe encontrar el código único (hash) que identifica ese bloque, mediante un proceso de prueba y error (PoW).

Una vez obtenido, se comunica la solución a la red, los demás mineros proceden a su verificación y, posteriormente, se incorpora a la blockchain. Este proceso de validación transaccional, realizado mediante los mecanismos de consenso llevados a cabo por los mineros, resulta en la emisión de nueva moneda.

**Figura 1**. Cadena de firmas digitales en transacciones de Bitcoin.




**Fuente**: Blockchain: la revolución industrial de internet.

Respecto al funcionamiento y la implantación de las criptomonedas, ambos se realizan mediante la tecnología cloud computing, la computación de altas prestaciones y la criptografía.

El **cloud computing**, también conocido como informática en la nube, es un modelo a través del cual las empresas y particulares pueden acceder a servicios y recursos informáticos de manera remota a través de la web. Estos recursos incluyen servidores, almacenamiento, bases de datos, software y redes, entre otros; por lo que se trata de una entrega de servicios informáticos que ha transformado la forma de acceso y uso de la tecnología, ofreciendo flexibilidad, escalabilidad y eficiencia en costos. Las criptomonedas y el cloud computing son dos tecnologías que, aunque son independientes entre sí, están relacionadas en los siguientes aspectos:

1. Minería de criptomonedas en la nube, puesto que algunos mineros de criptomonedas optan por usar servicios de cloud computing para alojar su infraestructura de minería en lugar de comprar y mantener *hardware* especializado, lo cual les permite escalar sus operaciones de minería más fácilmente y pagar únicamente por los recursos utilizados.

2. Nodos de criptomonedas en la nube. Los participantes en algunas redes de criptomonedas, como Bitcoin o Ethereum, pueden ejecutar nodos completos para validar transacciones y contribuir a la seguridad de la red. Algunos usuarios optan por alojar dichos nodos en entornos de cloud computing debido a su disponibilidad y capacidad de escalabilidad, refiriéndose ésta a la capacidad de una red blockchain o plataforma de criptomonedas para manejar un mayor número de transacciones y usuarios a medida que crece y se expande.

3. Almacenamiento seguro. Algunos servicios de almacenamiento en la nube ofrecen opciones de almacenamiento cifrado que pueden utilizarse para resguardar las claves privadas de criptomonedas de manera segura.

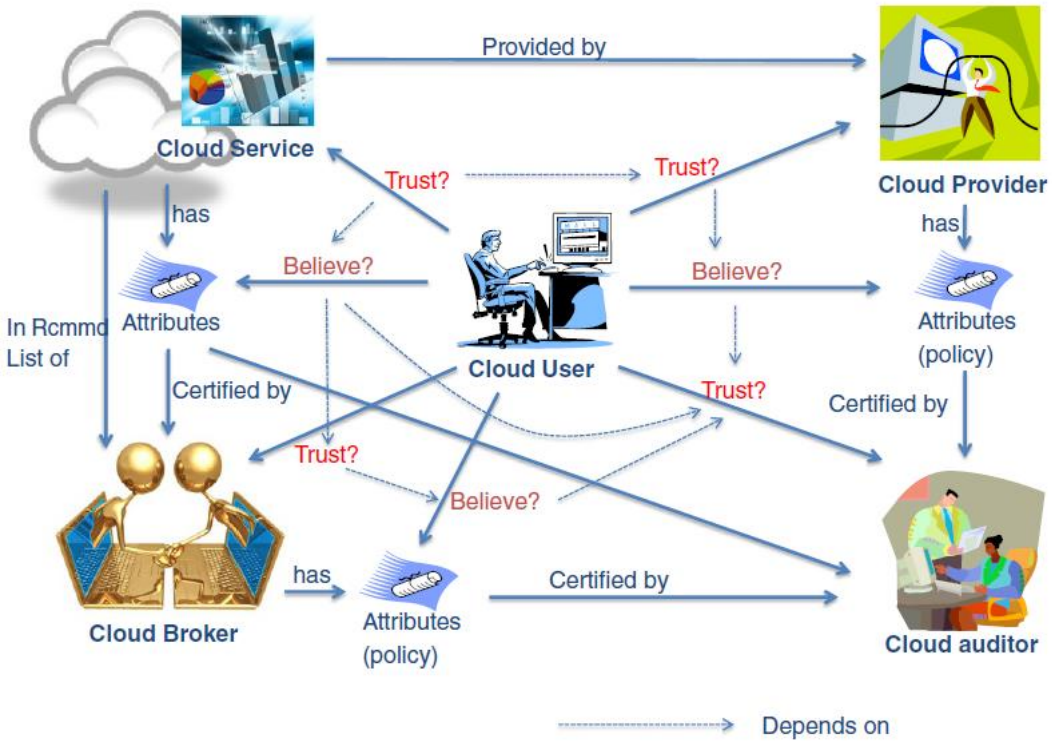
4. Desarrollo de aplicaciones blockchain. Los desarrolladores de estas aplicaciones pueden utilizar servicios en la nube para alojar nodos, bases de datos y aplicaciones descentralizadas (dApps).

5. Blockchain como servicio (BaaS). Algunos proveedores de servicios en la nube, como Microsoft Azure y Amazon Web Services (AWS), ofrecen soluciones de blockchain como servicio que permite a las empresas crear y gestionar fácilmente redes blockchain privadas o implementar tecnología blockchain en sus aplicaciones.

6. Transacciones de pago. Algunos proveedores de servicios en la nube aceptan pagos en criptomonedas, lo cual permite a los usuarios utilizar sus monedas digitales para pagar por servicios de almacenamiento de datos y otros servicios relacionados con la informática en la nube.

Cabe destacar que, si bien la informática en la nube proporciona una infraestructura flexible y escalable que puede ser útil para proyectos relacionados con criptomonedas y blockchain, también es importante abordar consideraciones de seguridad y privacidad al almacenar y gestionar activos digitales en ésta. Respecto a los mecanismos de confianza en la nube, los atributos de un servicio en ésta (o de su proveedor) se utilizan como prueba para el juicio de confianza del usuario sobre el servicio (o proveedor), y la creencia en dichos atributos se basa en certificaciones oficiales y cadenas de confianza para su validación.

**Figura 2**. Cadenas de relaciones de confianza en la nube.




**Fuente:** Huang and Nicol *Journal of Cloud Computing: Advances, Systems and Applications* 2013, 2:9

Esta figura proporciona una imagen integrada para ilustrar las cadenas de relaciones de confianza desde un usuario de la nube a un servicio en la nube y las entidades relacionadas en ésta, donde la acreditación se omite para simplificar.

Las relaciones de confianza con diversas entidades de la nube, mostradas en la parte izquierda de la figura, dependen de diversas fuentes de evidencia, que se muestran en la parte derecha, y todas esas relaciones de dependencia forman las cadenas de confianza (Huang, J., ¬ Nicol, D. 2013).

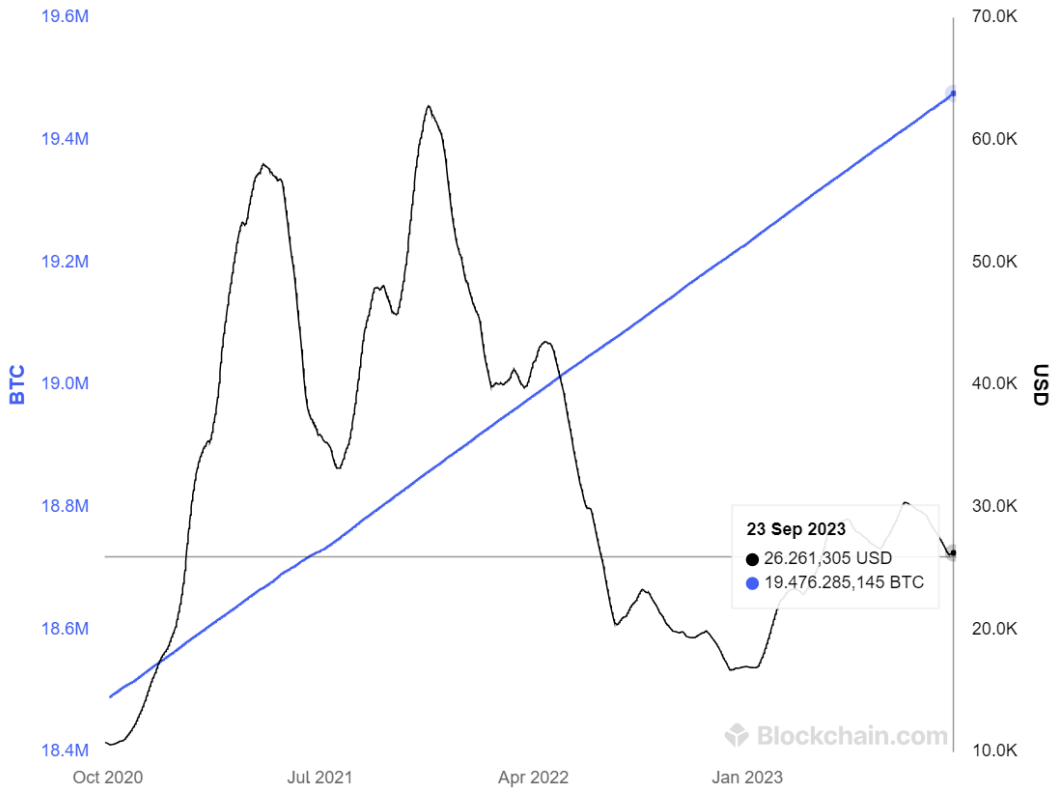
Respecto a la **computación de altas prestaciones**, también conocida como HPC (High-Performance Computing), se refiere a la utilización de sistemas de computación avanzados y altamente especializados para realizar tareas de procesamiento de datos extremadamente intensivas en cuanto a potencia de cálculo y velocidad. Su objetivo principal radica en la resolución de problemas complejos y demandantes que generalmente están fuera del alcance de las computadoras convencionales debido a su capacidad limitada de procesamiento y memoria.

La computación de altas prestaciones (HPC) y las criptomonedas están relacionadas en el contexto de la minería de criptomonedas en el cual los mineros necesitan un poder de procesamiento significativo y recurren a la HPC para lograrlo, especialmente en lo que respecta a las criptomonedas basadas en algoritmos de prueba de trabajo (PoW) cuyo proceso es intensivo en términos de recursos computacionales y energía.

## 2.1. Economía de las criptomonedas

En la actualidad existen 2177 criptomonedas. Sin embargo, la criptomoneda Bitcoin consta de una mayor importancia debido que fue la primera moneda virtual en crearse y, actualmente, es el activo más conocido y cotizado en el mercado de las criptodivisas. Es por esto que se trata del criptoactivo del que pueden extraerse mayores datos e información, por lo que las figuras representadas en los siguientes apartados son concretamente sobre la denominada *criptodivisa reina* por muchos a través de la cual es posible conocer de igual manera las diferentes situaciones de las demás criptomonedas.

**Figura 3**. Número de Bitcoins emitidos hasta septiembre de 2023.




**Fuente**: Blockchain.com

A 23 de septiembre de 2023, se habían generado un total de 19.476.285 Bitcoins. Sin embargo, debe matizarse la creencia en que parte de los Bitcoin puestos en circulación se han perdido o no pueden gastarse debido a la pérdida de contraseñas, errores en las direcciones de destino o fallos en los scripts de transacción, tal como indica Blockchain.com. Esto es debido a que los primeros participantes en el proyecto Bitcoin no efectuaron copias de seguridad de sus monederos electrónicos o perdieron sus claves privadas, especialmente durante los inicios de la criptomoneda cuando su valor de mercado era comparativamente bajo frente a las monedas fiduciarias.

El suministro total de Bitcoin está limitado y fue preestablecido en el protocolo Bitcoin a un máximo de 21 millones, con una recompensa por minería que decrece progresivamente con el tiempo. Esta política define cómo se generan los nuevos Bitcoins y el gráfico en cuestión ilustra la cantidad de Bitcoins que han sido minados o están en circulación hasta la fecha mencionada.

Adicionalmente, como indica el blog Bit2me Academy, se anticipa que a medida que el número de Bitcoins se aproxime al límite de 21 millones, la economía de Bitcoin experimentará una deflación, lo que significa que el poder adquisitivo de Bitcoin se incrementará hasta alcanzar un estado de estabilidad.

### 2.1.1. La deflación en las criptomonedas

La economía se caracteriza por experimentar dos fenómenos cíclicos que afectan directamente el valor de los bienes y servicios y la potencia de compra del dinero fiduciario: la inflación y la deflación. Durante un ciclo inflacionario, el precio de los bienes y servicios aumenta, llevando a una disminución en el valor del dinero fiduciario. Por el contrario, en un contexto deflacionario, se observa una disminución en los precios de los productos, lo que resulta en un incremento en el valor del dinero fiduciario. En períodos deflacionarios, los consumidores disfrutan de un mayor poder adquisitivo, pudiendo comprar una cantidad mayor de bienes y servicios por un costo inferior, mientras que la inflación representa el escenario opuesto.

En el ámbito de las criptomonedas se identifican tres factores primordiales que predisponen a estas divisas digitales hacia la deflación: el primero es el tope máximo predeterminado en la cantidad de monedas que pueden ser emitidas, como se mencionó previamente; el segundo, la reducción del 50% en la recompensa obtenida por los mineros por la validación de bloques cada cuatro años, un evento conocido como *halving*; y, el tercero, la tendencia al acaparamiento de dichas criptomonedas.

A lo largo del tiempo, se han registrado significativos incrementos en el precio de Bitcoin, que suelen ser seguidos por períodos de acaparamiento motivados por una euforia colectiva. Estos periodos de apreciación sostenida suelen ser breves y dan paso a fases prolongadas de depreciación en el valor de la criptomoneda, a menudo de manera acentuada.

Estas fases de deflación en el valor de Bitcoin implican que, con el tiempo, cada unidad de esta criptomoneda tiende a incrementar su valor, reflejando un aumento en el poder adquisitivo relativo de cada criptoactivo.

### 2.1.2. Adquisición de criptomonedas

La valoración de las criptomonedas se ve impactada significativamente por su nivel de adopción y las prácticas de acumulación o conservación. Los operadores de minería suelen comercializar la porción de criptoactivos necesaria para satisfacer los gastos operativos esenciales, que incluyen electricidad, mantenimiento y adquisición de equipo nuevo. La fracción remanente de monedas virtuales frecuentemente se retiene como una inversión a largo plazo, con la expectativa de que su valor aumente en el futuro (Ayala, G., 2018, 1 de noviembre).

**Figura 4**. Capitalización de mercado hasta septiembre de 2023.


**Fuente**: Blockchain.com

El valor total de mercado de la oferta circulante de una criptomoneda es similar a la capitalización de flotación libre en el mercado de valores, es decir, capitalización de mercado = Precio actual x Suministro en circulación.

La capitalización de mercado expuesta en la figura 4 representa el precio por el que se puede vender, concretamente, 1 Bitcoin. Es sabido que la oferta de estos es limitada lo cual significa que el precio es sensible a los cambios en la oferta y demanda.

La Figura 4 ilustra la trayectoria del valor de mercado, calculado mediante la multiplicación del número total de Bitcoin en circulación por su precio unitario. Como se detalla en el gráfico, la capitalización de mercado de Bitcoin permaneció relativamente estable hasta el año 2013. Posteriormente, en 2014, experimentó un modesto incremento, si bien el valor experimentó una declinación durante 2015, manteniéndose relativamente estable con leves oscilaciones hasta el año 2017. Fue en este último cuando la cotización de Bitcoin respecto al dólar experimentó un significativo aumento, alcanzando su máximo histórico. Este comportamiento resalta la pronunciada volatilidad que caracteriza al valor de Bitcoin en el período comprendido entre 2017 y 2019.

Respecto al periodo 2019-2021, la volatilidad del Bitcoin puede explicarse mediante factores y eventos que contribuyeron a los movimientos significativos de su precio tales como los ciclos del mercado de criptomonedas. El año 2019 comenzó con una fase de acumulación, seguida por un aumento significativo de precios a finales de 2020 y principios de 2021. Es sabido que, durante los ciclos alcistas, la volatilidad tiende a ser más pronunciada debido a la especulación y la entrada de nuevos inversores.

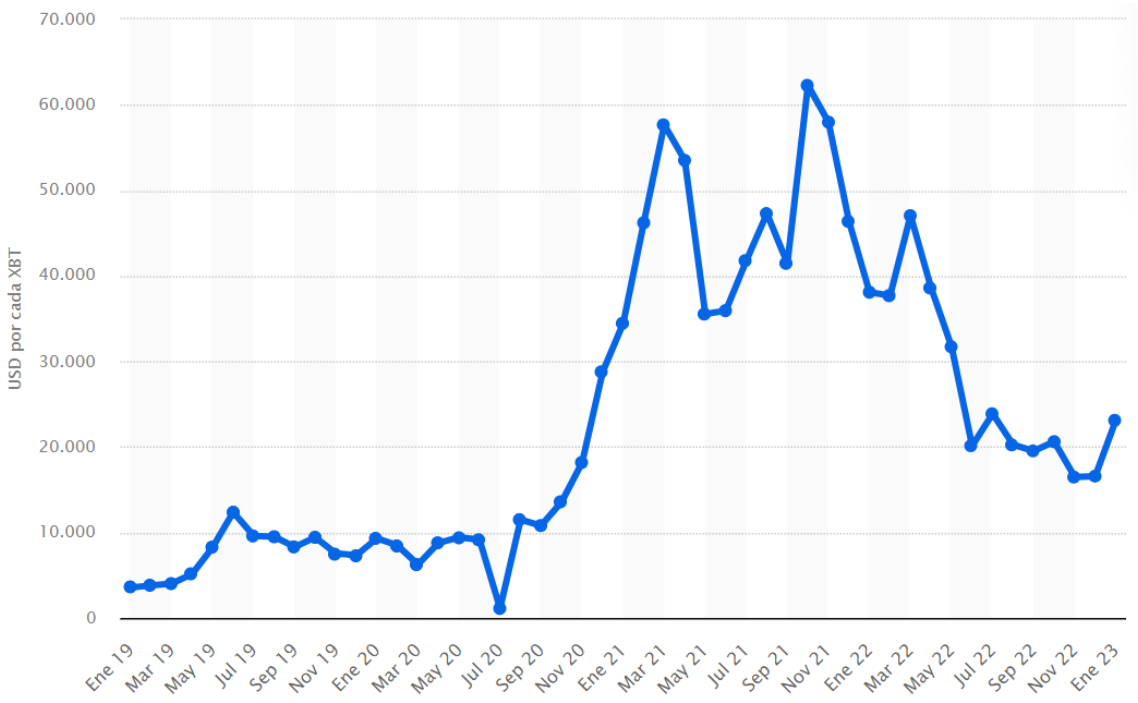
Durante dicho período, se observó un aumento en la adopción institucional de Bitcoin. Grandes empresas como Tesla y fondos de inversión como Grayscale Investments o Fidelity Digital Assets anunciaron inversiones en Bitcoin, lo que aumentó la legitimidad de la criptomoneda como una clase de activo lo cual contribuyó a su volatilidad.

La pandemia de COVID-19 y las respuestas económicas de los gobiernos y bancos centrales de todo el mundo tuvieron un impacto en los mercados financieros, incluido el mercado de criptomonedas; y en mayo de 2020, Bitcoin experimentó su tercer *halving* lo cual influyó en la oferta y la demanda puesto que se redujo la tasa de creación de nuevos Bitcoins, lo cual ha coincidido históricamente con aumentos en el precio.

Las noticias relacionadas con la regulación gubernamental y las prohibiciones de Bitcoin en ciertos países también tuvieron un impacto en su volatilidad. Además, los eventos de hackeos a intercambios y carteras que resultaron en la pérdida de fondos y datos de los usuarios afectaron la confianza en la seguridad de las criptomonedas destacando los riesgos de seguridad asociados con el almacenamiento y la gestión de estas tal y como sucedió con Binance y Upbit en 2019, KuCoin, Bitfinex y Ledger en 2020 y Cream Finance y Poly Network en 2021.

Durante las primeras semanas de mayo de 2022, el sector de las criptomonedas experimentó un evento significativamente adverso conocido como el criptocrash o criptoinvierno, revelando la considerable inestabilidad inherente a estas divisas digitales. Este periodo se caracterizó por la evaporación de más de 50.000 millones de dólares en valor de mercado, precipitado en gran medida por el desplome de la stablecoin UST de Terra, junto con su token de gobernanza, LUNA. A medida que avanzaba el criptoinvierno, la situación se agravó por la caída de entidades que, hasta ese momento, eran consideradas pilares estables dentro del ecosistema criptográfico, incluyendo a Celsius y FTX, así como a instituciones financieras de renombre tales como Silicon Valley Bank, Silvergate Capital y Signature. La fluctuación adversa del mercado afectó significativamente a las criptomonedas con mayor capitalización, arrastrando consigo a otras divisas digitales en el proceso.

**Figura 5**. Evolución mensual del tipo de cambio del bitcoin con el dólar estadounidense desde enero de 2019 hasta enero de 2023 (dólares por bitcoin).




**Fuente**: Statista.

La dinámica de oferta y demanda determina el valor del Bitcoin en comparación con las monedas fiduciarias. A lo largo de 2022, se observó una pronunciada caída en el precio de esta criptomoneda, tal como se refleja en el gráfico correspondiente. Para diciembre de 2022, Bitcoin alcanzó uno de sus puntos más bajos, cotizándose a aproximadamente 16.500 dólares por unidad. Sin embargo, en enero de 2023, experimentó una recuperación, elevando su precio a 23.109,3 dólares.

La finalidad de las gráficas presentadas en este segmento es doble. Por un lado, evidencian el crecimiento tecnológico y de adopción desde su concepción. Por otro, al considerar variables adicionales como la cotización frente a otras divisas o la variabilidad en las transacciones, revelan una volatilidad extremadamente alta. Esta característica provoca que las criptomonedas sean percibidas como opciones poco fiables para el resguardo de valor, dificultando su potencial para que los inversores dirijan hacia ellas sus ahorros. Adicionalmente, la ausencia de un valor intrínseco y extrínseco, derivada de la falta de respaldo por parte de cualquier entidad reguladora, complica en mayor medida su capacidad para cumplir con las funciones tradicionales del dinero, según Nieto Giménez-Montesinos y Hernáez Molera (2018).

### 2.1.3. Utilidad de las criptomonedas como medio de intercambio

Las criptomonedas constan de varias utilidades como medios de intercambio en transacciones económicas, destacando entre ellas la reducción de los costes asociados a servicios bancarios, un incremento en la eficiencia, la naturaleza de código abierto de su tecnología, y su resistencia a la falsificación, lo que incrementa su fiabilidad en este aspecto. Adicionalmente, la ausencia de regulación por parte de autoridades centrales impide el control sobre su valoración (Tristán Rodríguez, P., Guevara Segarra, M. F., & Cortez Alejandro, K. A., 2019, 31 de julio).

Otro aspecto importante a destacar sobre las criptodivisas es que éstas nunca cierran, es decir, es posible comprar o vender Bitcoin en cualquier momento y día, incluso durante la noche o los domingos y festivos. Esto aumenta la sensibilidad en tiempo real de precios a los cambios en los acontecimientos exógenos, ya que pueden reaccionar más fácilmente, incluso cuando otros mercados de negociación estén cerrados (Frota Decourt, R., Chohan, U. W., & Perugini, M. L., 2017).

La discusión respecto si las criptomonedas constituyen medios de intercambio o de pago ha sido analizada por Nieto Giménez-Montesinos y Hernáez Molera (2018), quienes argumentan que clasificar una divisa digital como medio de pago implicaría necesariamente obtener una autorización previa para su circulación.

El Banco Central Europeo, por otro lado, describe a la criptomoneda Bitcoin en su sitio web como una unidad de valor digital susceptible de ser intercambiada de manera electrónica, sin considerarla una moneda en sí. Para esta institución, representa un medio de intercambio electrónico carente de respaldo, sin ninguna garantía de derecho de uso ni esfuerzos institucionales para preservar su valor. Además, no es ampliamente reconocido como un medio de pago y se caracteriza por su extrema volatilidad. Finalmente, el Banco Central Europeo enfatiza que Bitcoin debe ser visto como un activo especulativo que conlleva un alto riesgo, especialmente dada la falta de regulación.

Para evaluar la viabilidad de las criptomonedas como forma de dinero, es esencial examinar si satisfacen las funciones fundamentales del dinero, las cuales incluyen:

- Ser un medio de cambio universalmente aceptado para bienes y servicios.
- Actuar como un depósito de valor, conservando poder adquisitivo a lo largo del tiempo.
- Funcionar como unidad de cuenta, proporcionando un estándar común para valorar y tasar productos.

Las objeciones principales hacia las criptomonedas resaltan que estas no cumplen o solo satisfacen parcialmente los tres criterios esenciales para ser clasificadas como dinero, lo cual sugiere que deberían ser consideradas como activos intangibles (Puyod, S. 2019-2020).

De acuerdo con la definición contenida en el artículo 4, apartado 25, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, al categorizar a las monedas virtuales primordialmente como un medio de cambio y no como un medio de pago, y al excluirles expresamente el estatus legal de moneda o dinero, se subraya la ausencia de una característica esencial del dinero fiduciario: su capacidad de extinguir deudas por parte de su poseedor.

Según lo discutido por Nieto Giménez-Montesinos y Hernáez Molera (2018), las monedas virtuales buscan desempeñar, hasta cierto punto, las funciones tradicionalmente atribuidas al dinero (actuar como medio de intercambio, depósito de valor y unidad de cuenta), pero actualmente solo alcanzan estos propósitos de forma muy restringida. Estas monedas están concebidas para operar como medio de intercambio dentro de ciertos contextos específicos y pueden, igualmente, actuar como vehículos para "almacenar" valor. A este efecto, poseen una naturaleza homogénea o fungible y son divisibles sin depreciación de su valor, similar al dinero en efectivo.

No obstante, a pesar de las intenciones de sustituir al dinero convencional que puedan manifestar, empezando por su denominación potencialmente engañosa («monedas»), no se les puede considerar como dinero ni es previsible que en el futuro lleguen a suplantar al dinero fiduciario, dado el conjunto significativo de restricciones que caracterizan su diseño.

## 2.2. Tipos de criptomonedas

Debido a los progresos tecnológicos y a la expansión global de los mercados financieros, se han introducido en circulación diversas criptomonedas, incluyendo Bitcoin, lanzado en 2009, y Ethereum, presentado en 2015, junto con numerosas otras que han emergido posteriormente.

### 2.2.1. Bitcoin

Durante la década de los ochenta, hubo esfuerzos significativos por desarrollar un sistema de pagos descentralizado, lo cual eventualmente condujo a la creación de Bitcoin. Sin embargo, esta criptomoneda no se materializó hasta el 3 de enero de 2009, en un contexto marcado por una crisis financiera que afectaba a las economías occidentales, provocando un profundo descontento entre la población. Este período coincidió con intervenciones significativas por parte de las autoridades monetarias, como la Reserva Federal de Estados Unidos y el Banco Central Europeo, mediante programas de liquidez que influyeron en los tipos de cambio de las monedas tradicionales y contribuyeron a una creciente desconfianza en el sistema financiero. En este contexto de dificultades financieras, surge Bitcoin como una moneda virtual descentralizada, atrayendo a un número creciente de seguidores debido a su naturaleza no regulada por ninguna entidad centralizada (Tristán Rodríguez, P., Guevara Segarra, M. F., & Cortez Alejandro, K. A. 2019, Julio 31).

Bitcoin se distingue por ser la primera criptomoneda en ser desarrollada, atribuida a un individuo o grupo de individuos que operaban bajo el seudónimo de Satoshi Nakamoto, cuya identidad real detrás de este nombre permanece desconocida, a pesar de que en 2008 se publicó el protocolo que daría origen a Bitcoin.

El sistema de Bitcoin atrajo la atención de Hal Finney, un destacado informático, matemático y criptógrafo reconocido por su contribución en la revisión del programa de cifrado Pretty Good Privacy (PGP). Este software, creado por Phil Zimmermann en 1991, fue diseñado para asegurar la privacidad de datos y comunicaciones vía correo electrónico mediante el uso de claves de cifrado de 128 bits, ofreciendo un nivel de seguridad comparable al empleado en ámbitos militares. La legislación de Estados Unidos, en aquel tiempo, clasificaba las claves de cifrado superiores a 40 bits como material de munición, lo que en 1993 llevó a una investigación penal contra Zimmermann por exportar PGP sin la licencia adecuada. Este contexto impulsó a colaboradores como Hal Finney a mantenerse en el anonimato hasta la conclusión de la investigación, evitando así posibles repercusiones legales (Frota Decourt, R., Chohan, U. W., & Perugini, M. L., 2017).

El año 2009 marcó el lanzamiento de Bitcoin Core, el primer software que dio origen a la red Bitcoin y sentó las bases para el desarrollo de futuras criptomonedas. La primera transacción con Bitcoin se efectuó en enero de ese mismo año entre Satoshi Nakamoto y Hal Finney, quien más tarde confesaría que nunca había conocido personalmente a Satoshi ni tenía conocimiento de su verdadera identidad. En 2010, Satoshi Nakamoto desapareció de manera abrupta dejando el desarrollo de Bitcoin en manos de otros desarrolladores y miembros de la comunidad.

De acuerdo con Vásquez Leiva (2014), Bitcoin se caracteriza por ser un sistema de intercambio electrónico basado en un protocolo específico y una red de ordenadores interconectados. Por otro lado, The Bitcoin Foundation lo define como un innovador sistema de pagos y una divisa digital en su totalidad. Bitcoin se distingue por ser una red de consenso que opera como la primera en permitir pagos directos entre partes, facilitando transacciones de comprador a vendedor sin la necesidad de intermediarios, bajo un esquema descentralizado, impulsado por los propios usuarios y sin la existencia de una autoridad central que lo regule. Dicho sistema incorpora una metodología contable denominada "contabilidad triple", que, además de registrar las operaciones en el debe y el haber, como en la contabilidad doble, introduce un tercer registro. Arjona (2013) detalla que esta tercera entrada registra y evalúa el impacto de las transacciones en los flujos de fondos, afectando así el estado de flujos de efectivo. Por tanto, en este modelo de contabilidad triple, no solo se coordinan los dos componentes fundamentales de un evento contable — el origen o fuente de financiación, reflejada en el haber, y el uso o inversión, que se registra en el debe —, sino que también se incluye una tercera dimensión que representa el movimiento de los flujos de efectivo.

La metodología de la contabilidad triangular cumple con una función bifronte. En un primer nivel, esta metodología permite visualizar el flujo de operaciones en el mismo acto de registro contable, y, en segundo término, favorece la generación del estado de flujo de efectivo mediante la agregación de los saldos de cuenta, otorgando así un control ampliado sobre las transacciones ejecutadas con Bitcoin al evidenciar los movimientos de flujos y proveer datos relevantes y de gran utilidad.

Bitcoin emplea el proceso conocido como función hash, mencionado previamente, para validar y registrar las transferencias. Sin embargo, este sistema posee ciertas restricciones, como el hecho de que la función hash es unidireccional, lo cual significa que, aun disponiendo del resultado, no es posible deducir el dato original, confiriendo a Bitcoin una naturaleza pseudoanónima.

En lo que respecta a la cadena de bloques, esta actúa como un archivo maestro que registra todas las transacciones ejecutadas desde el inicio de Bitcoin, determinando el volumen de dicha criptomoneda acumulado en los monederos electrónicos. Avanzando en la estructura de la blockchain, se encuentra el concepto de "marca de tiempo" (Time-stamp), el cual se describe como un procedimiento para situar un documento digital en un momento específico, autenticar un contrato o verificar una transacción ejecutada electrónicamente. Dicho concepto es utilizado para reforzar la seguridad en las transacciones. Finalmente, se introduce el término "prueba de trabajo" (proof-of-work), el cual se refiere a un protocolo de seguridad para los bloques. En este sistema, el usuario interactúa con el servidor para acceder a un servicio. Seguidamente, el servidor plantea un desafío que el usuario debe resolver. Una vez que el servidor verifica la correcta solución del desafío, concede el acceso al servicio (González Medina, R., 2019, Junio).

### 2.2.2. Ethereum

La moneda digital Ether se originó en el contexto de Ethereum, una plataforma de blockchain de código abierto presentada inicialmente en 2013 por Vitalik Buterin, un prominente investigador y desarrollador en el ámbito de las criptomonedas.

La finalidad de Ethereum radicaba en ofrecer una versión avanzada y ampliada de la criptomoneda Bitcoin. La recaudación de fondos para el desarrollo del software de Ethereum se llevó a cabo mediante una oferta inicial de moneda (ICO) en línea entre julio y agosto de 2014, y la plataforma fue lanzada oficialmente el 30 de julio de 2015. Al inicio, se pusieron a disposición para la venta pública inicial un total de 11.9 millones de monedas, lo que representaba cerca del 13% de su suministro circulante en aquel momento.

Tal y como expone Preukschat, la Fundación Ethereum representa un caso destacado de las capacidades innovadoras de la tecnología blockchain, especialmente en lo que respecta a la implementación de contratos inteligentes en cadenas de bloques públicas. Esto ha posibilitado nuevas formas de financiamiento, como el crowdfunding para proyectos de desarrollo de productos, así como la venta de acciones virtuales o la subasta de lotes de productos a través de contratos inteligentes. De este modo, Ethereum ha introducido métodos renovados para la ejecución de financiamientos, compras de participaciones o procedimientos de subasta.

Dentro del ámbito de las criptodivisas, se emplea un mecanismo denominado Oferta Inicial de Moneda (ICO, por sus siglas en inglés, Initial Coin Offering) o venta de tokens, que desempeña un papel fundamental en la financiación de la creación de nuevos protocolos digitales. Los inversores especializados en ICOs investigan y monitorean el lanzamiento de nuevas criptomonedas con el objetivo de anticiparse a posibles tendencias en el mercado.

Estos inversores pioneros procuran capitalizar la potencial apreciación de valor del token en cuestión tras su introducción exitosa en el mercado. Por lo tanto, la ICO representa una modalidad de captación de recursos similar a las ofertas públicas iniciales (OPI) en el mercado de valores, aunque se diferencia por emanar de un entorno descentralizado y carecer de un marco regulatorio y legal establecido. Entre los ejemplos más destacados de ICOs en el sector de las criptomonedas se encuentra el asociado al protocolo de Ethereum. Durante su campaña de financiamiento en el verano de 2014, Ethereum logró recaudar 31.531 ethers, equivalentes a 15 millones de dólares en aquel momento, a través de un esquema de pre-minado en el cual los inversores se comprometieron a esperar un año antes de poder comercializar sus ethers en el mercado, una condición estipulada en el acuerdo de inversión de la ICO para limitar la especulación inicial.

En aquel entonces, el lanzamiento de Ether constituyó una de las iniciativas de financiamiento colectivo más exitosas jamás vistas en el ámbito de los protocolos digitales, consolidando a Ethereum y su criptomoneda asociada como competidores directos de Bitcoin. A partir de ese momento, varias de las Ofertas Iniciales de Moneda (ICO) más destacadas y significativas para protocolos descentralizados nuevos optaron por utilizar Ethereum como su protocolo de referencia. Un ejemplo notable ocurrió el 30 de abril de 2016, cuando la empresa emergente Slock.it, parte del ecosistema de Ethereum, anunció el lanzamiento de TheDAO. Esta campaña de financiamiento colectivo ofreció al público los tokens de DAO (Organización Autónoma Descentralizada) por primera vez, recaudando 12,07 millones de ETH (un equivalente a más de 150 millones de dólares). TheDAO se propuso como un fondo de capital de riesgo participativo, permitiendo a cualquier persona en el mundo invertir en proyectos que operaran sobre la base de Ethereum, automatizados mediante contratos inteligentes y sin requerir una estructura de gestión tradicional.

Sin embargo, TheDAO experimentó un revés significativo cuando un atacante logró inmovilizar 3,6 millones de ethers, desencadenando un "hard fork" que dividió a la comunidad de Ethereum en dos cadenas de bloques distintas: Ethereum (ETH) y Ethereum Classic (ETC). El término hard fork se refiere a un cambio fundamental y no compatible en el protocolo de una criptomoneda o una red blockchain. En este, se altera el código base de la cadena de bloques de manera que las versiones anteriores del software ya no son compatibles con la nueva versión. Como resultado, se crea una cadena de bloques separada y divergente a partir del punto de bifurcación, y los usuarios deben actualizar sus nodos y software para continuar participando en la red.

Esta crisis, sumada a dificultades técnicas adicionales, desencadenó una reducción en el valor de Ether, que pasó de alcanzar un pico de 21,50 dólares por unidad a mediados de junio de 2016, a descender hasta los 7 dólares hacia finales del mismo año. A pesar de este notable descenso, la valorización de Ether a lo largo de 2016 registró un incremento del 700%, según Preukschat, A. (2017).

En 2017, Ethereum ganó popularidad como plataforma para contratos inteligentes y aplicaciones descentralizadas (dApps). Numerosas ICOs se llevaron a cabo en la red Ethereum, lo que contribuyó al aumento de la demanda y el precio de ETH. En diciembre de 2020, se lanzó la Fase 0 de Ethereum 2.0, que introdujo la prueba de participación (PoS) en la red. Dicha fase es parte de un proceso gradual para migrar completamente a PoS y resolver de esta manera los problemas de escalabilidad.

El algoritmo de Prueba de Participación (Proof of Stake, PoS) constituye uno de los dos mecanismos de consenso más predominantes empleados en las tecnologías de cadena de bloques, siendo el otro algoritmo el de Prueba de Trabajo (Proof of Work, PoW). A diferencia del PoW, el PoS es un protocolo destinado a la validación y verificación de transacciones y a la incorporación de nuevos bloques al blockchain. Este sistema se caracteriza por fundamentarse en la propiedad y participación de los usuarios en la red mediante criptomonedas. Específicamente, premia a los tenedores de criptoactivos mediante la asignación progresiva de nuevas unidades de la misma criptomoneda, a través de un proceso que asemeja una lotería entre los poseedores de la moneda. Dentro de este modelo, es común que se lleven a cabo actividades de preminado por parte de los desarrolladores del protocolo, quienes distribuyen inicialmente una cantidad determinada de criptomonedas a un grupo selecto de inversores. Con la posterior apertura de la distribución al gran público, se busca incrementar el valor de la nueva criptomoneda para maximizar los beneficios, condicionado esto al éxito de las estrategias de marketing implementadas. Esta dinámica sugiere que los modelos basados en Prueba de Participación pueden ser susceptibles a manipulaciones y fraudes, a diferencia del modelo de Prueba de Trabajo, donde el control sobre la distribución de las monedas por parte de los creadores del protocolo es significativamente más limitado.

Respecto las finanzas descentralizadas (DeFi) y los tokens no fungibles (NFT), en 2021 Ethereum se convirtió en el epicentro del auge de estas en cuya red se lanzaron innumerables dApps y mercados NFT lo cual provocó un aumento significativo en el precio de Ethereum a lo largo de 2021, superando los $4,000 USD en mayo y alcanzando máximos históricos.

Una distinción clave entre Bitcoin y Ethereum reside en la naturaleza y funcionalidad de sus tokens. Mientras que en la red de Bitcoin el token principal es la criptomoneda en sí, Ethereum ofrece la capacidad de generar tokens personalizados dentro de su plataforma, los cuales pueden representar desde monedas alternativas hasta acciones de empresas. En este contexto, resulta imperativo asegurar la autenticación de las partes involucradas en la transacción, tanto del emisor como del receptor, así como establecer de manera clara la propiedad de los tokens y los mecanismos a través de los cuales se transfiere dicha propiedad.

## 2.3. Aspectos legales y regulatorios

Tal y como es expuesto por Nieto Giménez-Montesinos y Hernáez Molera (2018), las criptomonedas representan un desafío en términos de regulación, al no encuadrarse claramente dentro de las categorías existentes en el ámbito económico y jurídico. No obstante, presentan similitudes con la moneda fiduciaria, los sistemas de pago, y los instrumentos financieros, lo que ha generado un interés creciente por parte de los organismos reguladores y de supervisión; quienes buscan evaluar adecuadamente los riesgos asociados a las criptomonedas y, en su caso, adoptar medidas de mitigación a través de los instrumentos regulatorios a su disposición.

En España, la fiscalidad de las monedas virtuales está regulada por la Agencia Tributaria, donde son consideras un activo financiero por lo que deben ser declaradas en la declaración de la renta anual en el apartado correspondiente a "Ganancias y Pérdidas Patrimoniales". Las ganancias derivadas de la venta de criptomonedas están sujetas al IRPF. También, existe una reducción en el impuesto a pagar si se mantienen las monedas virtuales durante más de un año, conocido como la "regla de los 12 meses". Respecto la minería de criptomonedas, ésta se considera una actividad económica por lo que está sujeta a impuestos debiéndose declarar los ingresos obtenidos a través de la minería como ingresos adicionales en la declaración de impuestos.

Por otro lado, desde 2021, las entidades que ofrecen servicios de cambio de monedas virtuales y custodia de activos digitales están obligadas a proporcionar información sobre las transacciones de sus usuarios a la Agencia Tributaria.

En España, las entidades que mantienen operaciones de manera directa o indirecta con activos digitales, están obligadas a acatar la "Ley 10/2010, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo" así como la "Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales". Por otro lado, los adquirentes de criptoactivos en España se rigen por la normativa nacional, específicamente la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal. Esta legislación impone la obligación a los poseedores de criptominedas de declarar tanto los saldos poseídos en estas divisas como las transacciones efectuadas con ellas, incluyendo adquisiciones, ventas, intercambios, transferencias, y cualquier otro tipo de operación financiera realizada con dichos activos. Dentro de las reformas normativas instauradas por la mencionada ley, se encuentra la modificación a la Ley 58/2002, de 17 de diciembre, General Tributaria, la cual dispone que la posesión de criptoactivos en carteras digitales internacionales debe ser declarada como parte del patrimonio en la declaración del impuesto sobre la renta.

Asimismo, se han introducido cambios en la Ley 35/2006, de 28 de noviembre, que regula el Impuesto sobre la Renta de las Personas Físicas, cuya reforma legislativa impone a las entidades que proveen servicios vinculados con criptoactivos el deber de reportar a la Hacienda Pública las transacciones de compra, venta, intercambio y transferencia de criptomonedas. Dicho reporte debe incluir información detallada sobre las transacciones y las partes involucradas, incluidos sus domicilios, números de identificación fiscal, el tipo y volumen de criptoactivos transaccionados, así como el valor y la fecha de cada operación.

Respecto al Impuesto sobre el Valor Añadido, la Agencia Tributaria ha establecido que las transacciones de monedas virtuales no están sujetas a IVA en sí mismas con la excepción de las empresas que prestan servicios relacionados con criptomonedas, como la conversión de éstas en moneda fiduciaria, las cuales sí pueden estar sujetas al Impuesto.

La Agencia Tributaria, mediante la Consulta Vinculante V1029-15 del 30 de marzo de 2015, ha clarificado que las transacciones realizadas con criptomonedas están sujetas a un régimen fiscal específico. Se establece que estas operaciones se consideran exentas del Impuesto sobre el Valor Añadido (IVA), al equiparar la compraventa de monedas virtuales a una actividad económica. Esta interpretación surge al reconocer que dicha actividad implica la organización autónoma de recursos materiales y humanos, o de uno de estos, con el objetivo de participar en la producción o distribución de bienes o servicios. En particular, el caso examinado involucra a una entidad dedicada a la comercialización de moneda virtual mediante una plataforma en línea, obteniendo ingresos a través de comisiones, lo cual refuerza su carácter empresarial.

Por su parte, el Tribunal de Justicia de la Unión Europea, respaldando esta postura, ha reconocido la exención de IVA para las transacciones con criptomonedas bajo el marco establecido en el artículo 13, parte B, letra d), número 3, de la Sexta Directiva 2006/112/CE. Dicha directiva, que aborda los métodos de pago convencionales como los cheques, fundamenta su decisión en el principio de que las operaciones de transferencia de dinero no deben estar sujetas al IVA. Este criterio busca garantizar la neutralidad fiscal de las operaciones que implican la circulación de dinero, ya sea mediante transferencias bancarias directas o el uso de instrumentos financieros que sirven como mandatos de pago.

La normativa fiscal española, en la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas, establece en su artículo 33.1 los criterios para la identificación de las ganancias y pérdidas patrimoniales. Esta disposición legal define dichas ganancias y pérdidas como cambios en el valor del patrimonio del contribuyente que se evidencien a raíz de cualquier modificación en su composición, exceptuando aquellos casos que la misma Ley específica como rendimientos. Este marco legal es fundamental para la comprensión y correcta declaración de las variaciones patrimoniales en el contexto fiscal.

De acuerdo con el marco establecido en la "Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas", en particular el articulado en su sección 33.1, las variaciones en el valor del patrimonio del contribuyente que emergen de cualquier cambio en su estructura, salvo excepciones específicamente clasificadas por la ley como rendimientos, se consideran ganancias o pérdidas patrimoniales. En este contexto, la interpretación de las normativas fiscales aplicables a las transacciones con criptomonedas sugiere que cualquier ajuste en el valor del patrimonio derivado de estas operaciones debe ser evaluado de la siguiente manera:

- En la conversión de criptomoneda a moneda fiduciaria, se identifica una transformación en la estructura del patrimonio, caracterizada por la transición de activos de naturaleza diferente. Esta operación implica un ajuste en el valor del patrimonio, medido por la valoración contable (equivalente al valor de mercado de la criptomoneda en el momento de la transacción). Dicha variación es clasificada como una ganancia patrimonial, de acuerdo con lo estipulado en la mencionada ley del impuesto sobre la renta.

- En el intercambio de criptomonedas por bienes o servicios, se produce una alteración en la composición del patrimonio, debido a la diferencia en la categoría entre la moneda digital y el bien o servicio adquirido. Este proceso conlleva una modificación en el valor, que se calcula a partir de la comparación entre la valoración contable de la criptomoneda (costo de adquisición) y su valoración justa en el mercado (precio de cotización) al momento de la operación, correspondiente al valor del bien o servicio obtenido.

- En el canje de una criptomoneda por otra, se contempla igualmente una modificación en la estructura patrimonial, marcada por el cambio de un tipo de activo digital por otro. Este escenario implica una evaluación de las ganancias o pérdidas patrimoniales derivadas de la transacción, considerando las fluctuaciones en el valor de mercado de las criptomonedas involucradas desde la adquisición hasta el momento del intercambio.

En el contexto del marco normativo español, es relevante destacar que, a partir de una interpretación emitida en 2013 por el Instituto de Contabilidad y Auditoría de Cuentas, el bitcoin fue inicialmente categorizado como un activo circulante. No obstante, una subsiguiente interpretación proporcionada por la Dirección General de Tributos, fechada el 27 de marzo de 2015, propuso una perspectiva alternativa, sugiriendo que las monedas virtuales deberían ser consideradas como medios de pago. Esta interpretación especifica que, dadas sus características particulares, las monedas virtuales se encuadran dentro de la categoría de "otros efectos comerciales", y, por ende, las operaciones de venta de dichas monedas estarían sujetas y exentas del Impuesto sobre el Valor Añadido (IVA).

Desde la perspectiva contable, las transacciones realizadas con monedas virtuales son reconocidas mediante el registro de los correspondientes ajustes patrimoniales a través de la cuenta de pérdidas y ganancias. Cabe mencionar que, hasta la fecha, la legislación española no ha establecido disposiciones específicas relativas a esta materia, y tampoco se han presentado propuestas legislativas futuras al respecto.

Por otro lado, Alemania se destaca como un precursor en la regulación de las divisas digitales, habiendo adoptado medidas que, desde el año 2020, permiten a las entidades financieras ofrecer a sus clientes servicios de banca en línea que incluyen, además de los valores tradicionales como acciones y bonos, las criptomonedas. Esta legislación alemana introduce facilidades adicionales, tales como la ampliación de los plazos para la solicitud de las licencias necesarias, fortaleciendo así el marco regulatorio aplicable a estos activos digitales.

En la Unión Europea, las criptomonedas gozan de legitimidad legal, aunque no existe una legislación concreta que las defina como dispositivo monetario. Cabe destacar que el impuesto sobre las ventas (IVA/GST) no se aplica a las conversiones entre las monedas de la UE y las criptomonedas. En términos fiscales, las regulaciones fiscales tradicionales siguen siendo aplicables a las transacciones que involucran criptoactivos.

En octubre de 2015, el Tribunal de Justicia de la Unión Europea estableció que la conversión de monedas convencionales a bitcoins se encontraba exenta del Impuesto sobre el Valor Añadido (IVA), puesto que las criptomonedas debían tratarse como un medio de pago. El Banco Central Europeo (BCE), por su parte, sostiene que las regulaciones destinadas al sector financiero tradicional no son aplicables, dado que no existen intermediarios financieros convencionales involucrados, y califica a las criptodivisas como un tipo de convertible virtual descentralizado.

En el ámbito regulatorio europeo, se destaca la "propuesta de resolución del Parlamento Europeo sobre monedas virtuales (2016/2007(INI))", la cual define a las criptomonedas como una representación digital de valor que no es emitida por ningún banco central ni por autoridad pública alguna. Estas representaciones de valor están asociadas, pero no respaldadas directamente, por divisas fiduciarias, y son aceptadas tanto por individuos como por entidades jurídicas como medio de pago. Además, pueden ser transferidas, almacenadas o comercializadas electrónicamente. Esta definición subraya el uso de la tecnología de registro distribuido, también conocida como blockchain, como una base fundamental para estas monedas digitales, evidenciando la ausencia de una categorización uniforme a nivel global, lo que implica que las monedas virtuales se consideran de hecho como moneda digital.

Por otro lado, la Autoridad Bancaria Europea (EBA) proporciona una perspectiva similar, indicando que las monedas virtuales pueden ser entendidas como representaciones digitales de valor que no son producidas por un banco central ni por una autoridad pública.

Estas representaciones de valor, a pesar de no estar directamente vinculadas a monedas fiduciarias, son aceptadas como medios de pago por personas físicas y jurídicas, y pueden ser transferidas, almacenadas o negociadas electrónicamente. Esta concepción subraya la autonomía y la naturaleza descentralizada de las criptomonedas dentro del sistema financiero contemporáneo. A pesar de la ausencia de una entidad central que respalde la emisión de esta forma de moneda digital como un medio de crédito válido para transacciones, no se puede clasificar al dinero electrónico como moneda de curso legal.

Dentro del contexto de la Unión Europea, las orientaciones preliminares para los consumidores surgieron de los informes elaborados por la Autoridad Bancaria Europea (EBA) en julio de 2014 y por el Banco Central Europeo (BCE) en febrero de 2015. Estos documentos resaltaban los riesgos principales vinculados con el uso de las criptomonedas y la necesidad de establecer un marco normativo adecuado para su regulación. Posteriormente, el Tribunal de Justicia de la Unión Europea, mediante su fallo del 23 de octubre de 2015, reconoció al Bitcoin como una moneda virtual, legal y apta para ser utilizada en transacciones entre individuos y comercios, determinando además que las operaciones de intercambio de esta divisa por otras quedaban exentas del Impuesto al Valor Añadido (IVA).

En una fase más avanzada, el enfoque regulatorio respecto a las monedas virtuales se ha orientado primordialmente hacia la prevención de su uso en actividades de lavado de dinero y financiamiento del terrorismo. En particular, con la implementación de la Directiva (UE) 2018/843, de 30 de mayo de 2018 (conocida como 5AMLD), se extendió su aplicación para incluir a los proveedores de servicios de intercambio entre criptomonedas y monedas de curso legal, así como a los proveedores de servicios de custodia de monederos electrónicos.

Con el fin de combatir el lavado de activos, el acuerdo provisional alcanzado el 9 de marzo de 2019, y posteriormente ratificado en junio de 2022 por el Parlamento Europeo y el Consejo, el cual recibió la aprobación formal del Parlamento en abril de 2023 y del Consejo en mayo de 2023, por parte de los estados miembros de la Unión Europea, se orienta a garantizar la trazabilidad de las transferencias de criptoactivos. Así, siguiendo el modelo de supervisión aplicado a las transacciones financieras convencionales, las transferencias de criptomonedas serán objeto de seguimiento, permitiendo el bloqueo de transacciones que resulten sospechosas. Esta medida, conocida como la "regla del viaje", que ya se encuentra en uso dentro del sector financiero tradicional, estipula la necesidad de identificar tanto el origen de los fondos como al destinatario final en dichas transferencias. Este marco regulatorio se aplica a transacciones que excedan los 1.000 euros provenientes de carteras no custodiadas (es decir, direcciones de monederos electrónicos en posesión de individuos) que interactúen con carteras custodiadas administradas por proveedores de servicios de criptoactivos. Sin embargo, estas disposiciones no afectan a las transferencias realizadas directamente entre particulares sin la intervención de un proveedor, ni a aquellas operaciones realizadas entre proveedores que actúen en nombre propio.

En el marco de las estrategias implementadas para mitigar los riesgos asociados al blanqueo de capitales, el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, fechado el 31 de mayo de 2023, el cual se ocupa de la regulación de los mercados de criptoactivos y modifica los Reglamentos (UE) nº 1093/2010, (UE) nº 1095/2010, así como las Directivas 2013/36/UE y (UE) 2019/1937, establece que la Autoridad Europea de Valores y Mercados (AEVM) mantendrá un registro público de aquellos proveedores de servicios de criptomonedas que operen dentro de la Unión Europea sin la debida autorización y en incumplimiento de la normativa vigente.

La postura europea respecto a las divisas digitales y su tratamiento regulatorio presenta diferencias significativas en comparación con la perspectiva estadounidense. En Europa, son consideradas principalmente como una divisa, en contraste con Estados Unidos donde, según lo estipulado por la Commodity Futures Trading Commission, son clasificadas como una mercancía (commodity) y, por tanto, sujetas a la regulación aplicable a estos activos. Además, en el contexto estadounidense, algunos estados requieren licencias específicas para la supervisión de los mercados de monedas digitales, mientras que otros han propuesto restricciones al uso de estas monedas en determinadas áreas.

En el contexto global, instituciones como el Consejo de Estabilidad Financiera, el Comité de Supervisión Bancaria de Basilea, la Organización Internacional de Comisiones de Valores y el Comité de Pagos e Infraestructuras del Mercado (por sus siglas en inglés, FSB, BCBS, IOSCO y CPMI, respectivamente) están llevando a cabo un análisis exhaustivo sobre las monedas virtuales. En julio de 2018, el FSB, en coordinación con las instituciones previamente mencionadas, presentó un informe al G-20 enfocado en los criptoactivos, donde se evalúan los riesgos que estos pueden conllevar. El documento concluye que, aunque en el momento actual no constituyen una amenaza significativa para la estabilidad financiera global, es fundamental mantener una vigilancia constante sobre su desarrollo y elaborar métricas adecuadas para su seguimiento.

De este modo, pese a que las monedas virtuales fueron inicialmente ideadas como una alternativa de pago descentralizada y autónoma, la tendencia actual indica que están siendo adoptadas principalmente como instrumentos de inversión y especulación financiera.

## 2.4. Riesgos y desafíos

Siguiendo la exposición de Nieto Giménez-Montesinos y Hernáez Molera (2018), las criptomonedas plantean considerables riesgos para los consumidores, los cuales podrían resultar en perjuicios económicos para estos, y cuyos riesgos pueden resumirse de la siguiente manera:

- **Riesgos financieros**. Las divisas digitales se caracterizan por no poseer valor intrínseco, no contar con garantías legales ni estar respaldadas por instituciones, lo cual implica un riesgo de crédito significativo el cual surge debido a que, en situaciones de incumplimiento por una de las partes involucradas, el usuario no dispone de la protección que normalmente brindan los sistemas de pago reconocidos internacionalmente. La valoración de estas monedas se sustenta únicamente en la voluntad de otros usuarios de comprarlas, sujeta a variaciones de precio considerablemente volátiles que, en muchas ocasiones, no responden a fundamentos objetivos (riesgo de mercado). Además, la fijación de precios no es transparente y podría ser manipulada por las plataformas de intercambio. Los poseedores de estas monedas virtuales podrían enfrentar dificultades para convertirlas en moneda convencional cuando lo deseen (riesgo de liquidez), e incluso si tienen la posibilidad de venderlas, la transparencia en cuanto a las comisiones aplicadas podría ser insuficiente.

- **Riesgo operacional**, puesto que la tecnología que fundamenta la mayoría de las monedas virtuales aún se encuentra en una etapa de consolidación. Adicionalmente, la seguridad ofrecida por las plataformas que soportan dichas monedas no alcanza, en la actualidad, los niveles de seguridad característicos de los sistemas de pago tradicionales.

- **Riesgo de uso fraudulento y actividades ilícitas**. La naturaleza anónima o pseudónima de numerosas criptomonedas ha facilitado, en ciertos casos, su empleo en actividades ilícitas, tales como el blanqueo de capitales, la financiación del terrorismo, evasión fiscal, el comercio de mercancías prohibidas, extorsión y la solicitud de rescates mediante software de secuestro de datos (ransomware). Asimismo, se han utilizado para eludir controles de cambio y restricciones a los movimientos de capital en determinadas jurisdicciones.

- **Riesgo legal**, fundamentado en la ausencia de respaldo por un banco central o entidad reguladora reconocida. Debido a su naturaleza única, las criptomonedas no se ajustan claramente a las categorías legales establecidas, operando en un entorno sin regulaciones específicas ni supervisión oficial. Aunque actúan como instrumentos de intercambio, desde el punto de vista legal, frecuentemente no se reconocen como medios de pago convencionales, lo cual plantea desafíos en su clasificación y tratamiento legal. Como resultado, no se requiere una autorización específica para llevar a cabo transacciones con ellas, puesto que dicha actividad puede llevarse a cabo al margen del marco normativo que se aplica a las instituciones financieras.

En situaciones en las que se realice la compra de bienes y servicios utilizando monedas virtuales, los compradores pueden encontrarse en una posición vulnerable en términos de protección al consumidor en caso de enfrentar problemas relacionados con el pago, el producto adquirido o el servicio contratado. Actualmente, no existe un marco normativo exhaustivo que defina de forma abarcadora los derechos y responsabilidades de los usuarios de criptomonedas, incluyendo el derecho a recibir reembolsos ante transacciones erróneas o no autorizadas, y la obligación de asegurar la provisión de información clara y transparente.

El incremento en la popularidad de las criptomonedas, liderado por el bitcoin, sugiere un potencial aumento en los riesgos tanto para la estabilidad económica y financiera como para el conjunto de los consumidores. A pesar de que, hasta la fecha, se evalúa que los riesgos para la estabilidad del sistema monetario y financiero son contenidos, es crucial no subvalorar los riesgos a los que se exponen los consumidores, incluso en un contexto donde el uso de dichas divisas sigue siendo relativamente limitado.

El continuo avance de la tecnología, a su vez, facilita la aparición de nuevas técnicas cuyo objetivo es conseguir información a revelar de las cadenas de bloques. Algunas de estas amenazas son:

- **Ingeniería social:** Si se considera al usuario como el elemento más susceptible a riesgos, es pertinente reconocer el ambiente cotidiano en el que opera como la mayor fuente de amenazas. Plataformas como Facebook, Twitter, LinkedIn, entre otras, proporcionan a los actores maliciosos la capacidad de acceder a un volumen considerable de información personal, facilitándoles así la creación de estrategias de ataque más sofisticadas. Si un usuario comparte en alguna de estas aplicaciones una dirección que usa regularmente para realizar pagos, existe la posibilidad de rastrear movimientos de efectivo en una blockchain.

- **Servicios en la nube:** La infraestructura de la cadena de bloques se aloja en entornos de computación en la nube. Por consiguiente, cualquier vulneración en la seguridad de estos entornos podría potencialmente afectar la integridad de la cadena de bloques.

- **Bring Your Own Device** (BYOD): «Traiga su propio dispositivo» está estrechamente relacionado con el IoT (Internet of Things) y la concienciación de los usuarios sobre su percepción de la seguridad. En numerosos contextos organizacionales, se observa una creciente tendencia hacia la utilización de dispositivos informáticos que no son propiedad de la entidad, los cuales se encuentran interconectados con otros recursos que podrían resultar de interés para un potencial agresor. Por esta razón, la capacitación y la conciencia sobre la importancia de mantener actualizados y activos los sistemas de protección son fundamentales para los inversores en criptoactivos.

- **Factores de riesgo internos:** Los incidentes de seguridad descritos se originan no a través de actores malintencionados externos, sino mediante individuos que están integrados dentro de las propias organizaciones, quienes poseen un conocimiento detallado de las infraestructuras tecnológicas o aplicaciones en uso. La existencia de accesos ocultos (backdoors) en los sistemas posibilita la intrusión desde el exterior.

Cabe señalar que los ataques emblemáticos vinculados con esta tecnología ilustran de forma directa la importancia de implementar medidas de seguridad robustas en las soluciones que emplean tecnología de cadena de bloques. Aunque estas vulnerabilidades se han manifestado principalmente con el desarrollo de Bitcoin, representan desafíos de seguridad críticos que cualquier blockchain pública debe enfrentar y resolver adecuadamente:

- **Ataque de gasto duplicado**. Un ataque de gasto doble se produce cuando un agente logra hacer que el sistema reconozca como válidas dos transacciones distintas que utilizan la misma unidad de criptomoneda, configurando así un acto de fraude. Este tipo de ataque busca engañar al receptor de un pago, induciéndole a creer que ha recibido una transferencia de fondos a una dirección que controla, cuando en realidad los fondos han sido dirigidos a otra dirección bajo el control del atacante. A continuación, se describe el proceso de un ataque de gasto doble típico mediante una secuencia de eventos específicos:

    1. El agresor crea inicialmente una transacción, denominada $T_N$, que no será efectivamente recibida por el destinatario previsto. Acto seguido, genera una transacción fraudulenta, identificada como $T_F$, empleando las mismas entradas que en $T_N$ pero alterando las direcciones de destino a las controladas por él (C y D).

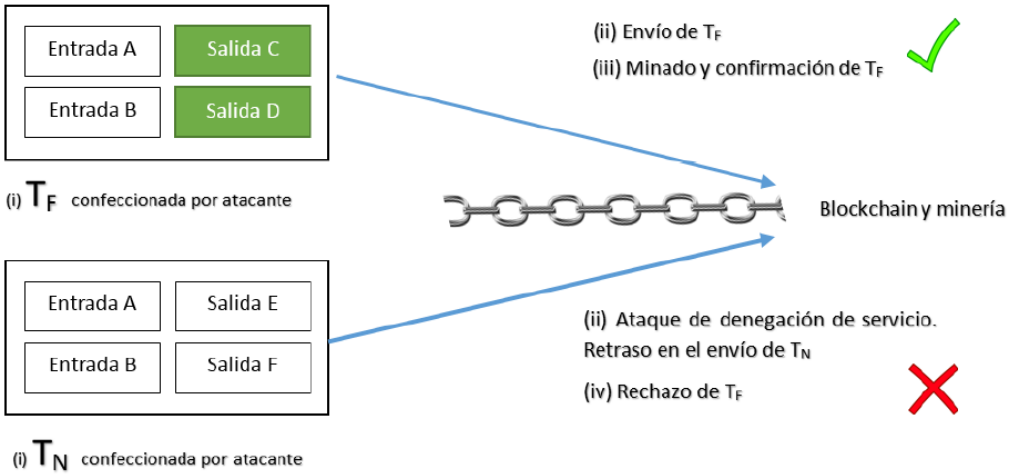
    2. El atacante posteriormente difunde la transacción fraudulenta $T_F$ a la red mientras simultáneamente lleva a cabo acciones para impedir la transmisión y confirmación de la transacción original $T_N$ mediante técnicas de denegación de servicio.

    3. Procede a participar en el proceso de minería con el objetivo de incorporar y validar la transacción fraudulenta $T_F$ dentro de la cadena de bloques.

    4. Cuando la red intenta procesar $T_N$, esta es rechazada de manera global puesto que la cadena de bloques está diseñada para no admitir múltiples transacciones que intenten usar la misma unidad de criptomoneda de forma concurrente.

En resumen, para que el ataque de gasto doble resulte exitoso, es crucial que la transacción fraudulenta $T_F$ sea confirmada con celeridad, mientras que $T_N$ sea sistemáticamente rechazada por la red.

**Figura 6**. Eventos de un ataque de gasto duplicado.




**Fuente**: Innovación disruptiva de las criptomonedas para la sociedad y el comercio electrónico.

- **El ataque del 51% en las blockchains públicas:** Para la ejecución de este ataque se requiere poseer el 51% del poder computacional de una red blockchain específica. La elección del 51% se debe a la capacidad de cálculo (hashrate) necesaria para falsificar la cadena de bloques. Para llevar a cabo un ataque exitoso que involucre la generación de bloques ilícitos, validación y su adición a la blockchain, resulta imperativo disponer de una capacidad de procesamiento computacional equivalente o superior a la del resto de participantes en la red. De esta manera, sería dicha cadena (y no otra) la que sería considerada como válida. Con tal poder, se podrían revertir transacciones, evitar confirmaciones deseadas, realizar ataques de doble gasto o llevar a cabo cualquier otra acción maliciosa. Este modelo de ataque representa una vulnerabilidad para cualquier infraestructura descentralizada que adopte el consenso Proof of Work (PoW) para la toma de decisiones. Un ejemplo notable de esta vulnerabilidad se manifestó en la red de Bitcoin Gold, la cual, a tres años de su lanzamiento, experimentó un ataque del 51%. Este incidente resultó en un doble gasto que excedió los 7.000 Bitcoin Gold ($BTG). Posteriormente, se sucedieron dos ataques adicionales en un lapso de seis horas, los cuales permitieron sustraer a los atacantes 1.900 y 5267 $BTG. Esto fue posible debido que su tasa de hash había caído hasta llegar casi a 0. Por ese motivo, el nivel de seguridad era inexistente y alcanzar el 51% de su tasa de hash era relativamente barato. En Ethereum Classic se han producido tres robos de este tipo junto con ataques de gasto duplicado. El último de ellos, en agosto de 2020, produjo un ataque que reorganizó más de 7.000 bloques. Anteriormente, sucedieron dos ataques adicionales en los que se tuvieron que reorganizar 3.693 y 4.000 bloques respectivamente a través de los cuales los ciberdelincuentes llegaron a sustraer más de 9 millones de dólares en transacciones de doble gasto.

- **La maleabilidad de las transacciones:** Implica la modificación del identificador de hash de una transacción que ha sido autorizada pero aún no confirmada, sin anular la firma digital asociada, de manera que la parte afectada asume erróneamente que el pago no se ha efectuado, a pesar de que en realidad sí se ha realizado. La transacción modificada se considera inválida bajo todas las circunstancias. No obstante, si esta versión alterada de la transacción alcanza a ser procesada por un nodo minero antes de la confirmación de la transacción legítima, entonces la versión fraudulenta quedará registrada en la cadena de bloques de los demás nodos. La finalidad de este ataque es desviar los fondos de la transacción hacia una cuenta bajo el control del atacante, quien, a diferencia de los escenarios de gasto doble, no es el creador original de la transacción sino el receptor que la altera. Un caso emblemático de esta vulnerabilidad se presentó en 2014, cuando MtGox, una destacada casa de cambio de bitcoins ubicada en Japón, anunció su bancarrota tras una pérdida de 500 millones de dólares (Decker & Wattenhofer, 2014). En una situación similar, FlexCoin, una plataforma de intercambio de bitcoins en Canadá, experimentó pérdidas de 600 mil dólares, lo que llevó a la terminación de sus operaciones (Rizzo, 2014).

Las criptomonedas permiten la transferencia a múltiples destinatarios prescindiendo de intermediarios bancarios o de entidades de control, facilitando su utilización como método de pago en diversas actividades ilícitas, como el blanqueo de capitales, el tráfico de drogas, el comercio ilegal de armas y otros actos delictivos.

En este escenario, emergieron diversas plataformas web que lograron obtener ganancias significativas, entre las cuales se destaca SilkRoad, un mercado en línea especializado en el comercio ilegal de sustancias estupefacientes. Para efectuar sus operaciones ilícitas, SilkRoad implementó un portal en la Dark Web y se apoyó en dos tecnologías fundamentales: TOR y Bitcoin. TOR se utilizaba para enmascarar la identidad de los usuarios, mientras que Bitcoin proporcionaba un mayor grado de anonimato al ser empleado como medio de pago. SilkRoad logró mantenerse en funcionamiento exitosamente hasta que su creador, quien se identificaba con el alias de Dread Pirate Roberts, fue detenido luego de que accidentalmente revelara su identidad real mediante un correo electrónico (Kethineni, S., Cao, Y., & Dodge, C., 2017).

# 3. PROBLEMÁTICA DE LAS PLATAFORMAS EXCHANGE

El uso de monedas virtuales como instrumentos de inversión ha experimentado un aumento significativo, a menudo impulsado por motivaciones especulativas. Sin embargo, resulta poco probable que se superen las limitaciones existentes en muchas de estas iniciativas en un futuro cercano. Estas limitaciones incluyen problemas de escalabilidad debido al elevado consumo energético en la producción de estas monedas, altos costos de transacción, desafíos de gobernanza y rigidez en su mecanismo de oferta.

Las criptomonedas están estrechamente ligadas a la tecnología. Durante la recuperación pandémica en 2021, caracterizada por la inyección de dinero barato en el mercado por parte de los bancos centrales, el sector tecnológico experimentó notables beneficios. Sin embargo, la situación macroeconómica ha experimentado cambios significativos, obligando a los bancos centrales a implementar aumentos sustanciales en las tasas de interés para contrarrestar el incremento generalizado de los precios. Estos incrementos en los tipos han llevado a los inversores a alejarse de los activos de mayor riesgo, optando en cambio por aquellos considerados más seguros, como los valores de renta fija. Como evidencia de este cambio, el Nasdaq ha experimentado una caída superior al 30% en lo que va del año, destacando la correlación entre el sector tecnológico y las criptomonedas.

Respecto a las *stablecoins*, término utilizado para describir un tipo particular de criptomonedas, estas están diseñadas específicamente para minimizar las fluctuaciones en su valor. Existen diversas estrategias para lograr esta estabilidad: algunas se asocian a monedas fiduciarias como el dólar o el euro, otras se respaldan con activos tangibles como el oro, algunas se basan en el valor de otras criptomonedas, como DAI, y finalmente, aquellas que regulan su precio mediante el uso de algoritmos, tal como sucede con UST (TerraUSD).

Con el objetivo de introducir estabilidad en el ámbito de las criptomonedas, Do Kwon diseñó TerraUSD en 2019, convirtiéndose en la *stablecoin* principal dentro del ecosistema Terra. TerraUSD (UST) buscaba mantener una paridad de 1:1 con el dólar estadounidense a través de su mecanismo algorítmico, utilizando su criptomoneda hermana, Terra (LUNA), para absorber las fluctuaciones de demanda. El mecanismo permitía a los usuarios intercambiar 1 dólar de UST por 1 dólar de LUNA y viceversa, con la intención de que la oferta y demanda controlaran la paridad de UST con el USD. Su valor se basaba en la expectativa de que los inversores capitalizarían las oportunidades de arbitraje, las cuales se presentan cuando existe una diferencia de precio para una misma criptomoneda entre diferentes plataformas. Así, la estrategia fundamental detrás de UST se apoyaba en la premisa de que los *traders* buscarían constantemente obtener ganancias de oportunidades de bajo riesgo.

El colapso de Terra (LUNA) y su *stablecoin* algorítmica TerraUSD (UST) en mayo de 2022 es uno de los eventos más notorios en la historia reciente de las criptomonedas puesto que supuso la liquidación de 30.000 millones de dólares en tan solo 7 días. Previamente, en los meses precedentes a mayo de 2022, la moneda experimentó un impresionante aumento de valor, aparentemente inmune a eventos globales como la invasión de Ucrania, la inflación y las fluctuaciones en los mercados de valores. Alcanzó su pico máximo en abril de dicho año, cotizando a 119,18 dólares por unidad de criptomoneda, lo cual representaba un incremento de mil veces su valor en tan solo dos años. Este incidente no solo resultó en pérdidas significativas para inversores y participantes del mercado, sino que también desencadenó un debate global sobre la regulación y la seguridad de las criptomonedas, especialmente las *stablecoins* algorítmicas.

Anchor Protocol, una plataforma DeFi construida sobre Terra por Terraform Labs, ofrecía unos rendimientos del 20% de APY (Annual Percentage Yield) por el depósito de UST, lo cual era insostenible a largo plazo. Este alto rendimiento impulsó la adopción del protocolo Anchor y sustentó la escalada en el precio de LUNA, que pasó de menos de $1 a principios de 2021 a $84 hacia finales de ese mismo año. Esto provocó dudas sobre la sostenibilidad de los altos intereses, llevando a los inversores a perder confianza en la capacidad de UST para mantener su paridad con el dólar.

La crisis de UST comenzó a gestarse cuando el 7 de mayo de 2022, se liberaron aproximadamente 2.000 millones de dólares del Protocolo Anchor, y de dicha suma, se vendieron inmediatamente cientos de millones. Esta venta en gran escala redujo el precio de UST a 0,91 dólares. Los inversores, buscando capitalizar la situación, intercambiaron UST a razón de 90 céntimos por cada dólar de LUNA. El mecanismo de estabilización de UST implicaba que, cuando su precio caía por debajo de 1 dólar, los usuarios podían quemar UST y crear LUNA, reduciendo así la oferta de UST y supuestamente ayudando a recuperar la paridad. Sin embargo, en Anchor solo se permite la "quema" de hasta 100 millones de dólares de UST por día, cuyo límite se alcanzó rápidamente, impidiendo que la *stablecoin* recobrara estabilidad a tiempo.

Los *traders* se dirigieron en gran número hacia otras plataformas y casas de cambio para convertir sus UST, resultando en un desequilibrio en el fondo de liquidez de Curve Finance, lo cual agravó la inestabilidad del precio. A medida que más UST se vendían y su precio comenzaba a caer significativamente por debajo de 1 dólar, el mecanismo diseñado para mantener la paridad se activó de manera excesiva, aumentando la oferta de LUNA drásticamente en un intento de absorber el exceso de UST. Sin embargo, la rápida y masiva impresión de LUNA causó una hiperinflación de la moneda, llevando su valor prácticamente a cero y erosionando la confianza en ambos activos, LUNA y UST.

Existe una teoría que sugiere que un inversor anónimo y adinerado tenía como objetivo realizar una venta en corto de Bitcoin mediante un ataque a Terra. Según esta teoría, la Luna Foundation Guard (LFG), establecida por los creadores de Terra para salvaguardar la *stablecoin*, había empezado a adquirir Bitcoin en volúmenes mayores para su reserva. La estrategia del atacante consistía en desestabilizar UST con el fin de obligar a los desarrolladores a liquidar sus bitcoins, provocando así una caída en su valor. La teoría especula que, de haberse llevado a cabo este plan, el atacante podría haber obtenido una ganancia de 800 millones de dólares.

El colapso de Terra y UST borró decenas de miles de millones de dólares en valor de mercado, afectando a un gran número de inversores. Además, este evento puso de relieve los riesgos asociados con las *stablecoins* algorítmicas, intensificando el debate sobre la necesidad de regulación y supervisión en el sector de las criptomonedas.

La implementación de medidas más estrictas en la política monetaria, las quiebras de algunos exchanges y los escándalos internos dentro del sector han exacerbado la pérdida de confianza entre numerosos inversores, lo que resultó en un colapso del valor de Bitcoin hasta los 17.000 dólares a mediados de junio de 2022. Esta caída representó una disminución de más del 75% con respecto a los máximos alcanzados en 2021. Desde entonces, el valor ha fluctuado en la zona de los 20.000 dólares por unidad.

Este evento ocurrió a raíz de los problemas experimentados por Celsius Network, una plataforma descentralizada y conforme a regulaciones destinada a los servicios de préstamo. Ofrecía a sus usuarios la oportunidad de ganar intereses sobre sus depósitos de criptomonedas, así como la posibilidad de pedir prestado utilizando sus criptoactivos como colateral, con un ratio de préstamo a valor (LTV) del 50% lo que significa que el usuario necesita depositar un valor superior al monto del préstamo solicitado como garantía. Originalmente, estas garantías se utilizaban para otorgar préstamos a entidades financieras, las cuales, a su vez, generaban intereses. Dichos intereses eran luego repartidos entre los usuarios que habían bloqueado (o "stakeado") sus criptomonedas en la plataforma.

La operativa de Celsius presenta paralelismos con la de un banco tradicional, en el sentido de que emplea los fondos de los usuarios para otorgar préstamos. A través de esta actividad, el banco produce intereses a partir de las operaciones financieras de los usuarios, al mismo tiempo que remunera a aquellos que han depositado sus activos en la plataforma.

En relación con el incidente en cuestión, los datos provenientes de la blockchain analizados por Nansen revelan que Celsius recurrió a múltiples protocolos dentro del ámbito de las Finanzas Descentralizadas (DeFi), incluyendo el Anchor Protocol, con la finalidad de maximizar los fondos de sus clientes y generar rendimientos que alcanzaban hasta un 18% de Tasa de Porcentaje Anual (APY).

Esta estrategia implicó la exposición a los riesgos inherentes a los contratos inteligentes, así como a potenciales fallos en el protocolo y a las fluctuaciones volátiles características del mercado.

Diversos expertos apuntan a que los contratiempos de Celsius comenzaron cuando el stETH, o ETH en staking, que se respaldaba en una proporción de 1:1 con Ethereum, perdió su paridad y sufrió un descenso significativo en su valor. El stETH se presenta como un activo que puede emplearse como colateral para obtener más ETH en ciertas plataformas DeFi. Por ende, cuando el stETH desvinculó su equivalencia con ETH, aquellas posiciones que habían obtenido ETH a través de préstamos usando stETH como garantía, fueron liquidadas, provocando una masificación de ventas de Ethereum impulsadas por el pánico en varios de los principales exchanges de criptomonedas.

La plataforma de préstamos descentralizados se encontraba en una posición en la que había asignado una porción significativa de los activos de sus clientes en stETH. La pérdida de la paridad de este último desencadenó una cascada de solicitudes de retiro que culminaron en una crisis de liquidez, exacerbada por el hecho de que Celsius constituía uno de los mayores detentores de stETH. Adicionalmente, la plataforma enfrentó adversidades financieras a raíz de la depreciación de LUNA y UST, teniendo aproximadamente 500 millones de dólares de los depósitos de clientes invertidos en Anchor Protocol. En este contexto, la entidad afrontó una merma de 120 millones de dólares de los recursos de sus usuarios.

La situación de crisis de liquidez se agudizó por una disparidad entre los pasivos y los activos líquidos disponibles. Se estima que el 73% de los ETH de Celsius estaban inmovilizados como stETH o comprometidos en staking en ETH 2.0, situación que restringía su disponibilidad hasta la ejecución de la denominada "fusión". Esta circunstancia colocó a Celsius en una posición de insolvencia respecto a su tenencia de ETH, dado que solo un 27% de su ETH se mantenía líquido. Paralelamente, el entorno de mercado propició retiros sustanciales de ETH, que escalaron hasta los 50.000 ETH semanalmente.

Adicionalmente a estos eventos, en junio de 2021, Stakehound, un proveedor de servicios de staking para Ethereum, comunicó la pérdida de las claves privadas correspondientes a más de 38.000 ETH. Según datos proporcionados por Nansen, se estima que Celsius experimentó una pérdida de aproximadamente 35.000 ETH en este incidente, resultando en la posesión de tokens de Stakehound que no poseían valor alguno. Durante este periodo, Celsius no comunicó a sus usuarios la mencionada pérdida. En una instancia posterior, la plataforma enfrentó pérdidas adicionales valoradas en 22 millones de dólares debido a una pérdida accidental de pagos de compensación asociados al incidente de seguridad de Badger DAO, de acuerdo con un análisis de cadena de bloques efectuado por Dirty Bubble Media. Las significativas retiradas de Ethereum provocaron un marcado descenso en el precio de ETH.

Paralelamente, el precio de Bitcoin, que hasta entonces había sostenido un nivel de soporte superior a los 28.000 dólares, experimentó una caída, perdiendo el soporte de los 20.000 dólares.

Este conjunto de circunstancias adversas contribuyó a la crisis de Celsius Network, la cual precedió a dificultades similares en otros protocolos y entidades de inversión dentro del sector, marcando uno de los episodios más turbulentos en la historia reciente del mercado de criptomonedas.

A partir de la primera semana de julio de 2022, Celsius inició el proceso de reembolso de una parte de los fondos que había tomado prestados. En dicho período, específicamente los días 1, 3 y 4 de julio de 2022, la plataforma repagó un total de poco más de 120 millones de dólares correspondientes a su deuda con Maker. Durante esos tres días, Celsius efectuó pagos de 60, 50 y 6,2 millones de DAI, completando así el reembolso total que finalizó el 8 de julio.

El 13 de julio de 2022, Celsius Network solicitó la protección por bancarrota bajo el Capítulo 11 de la Ley de Quiebras en el Tribunal del Distrito Sur de Nueva York. La naturaleza de la plataforma, que no está registrada como corredor de bolsa, impidió la opción de recurrir al Capítulo 7, que es más habitual en estas circunstancias. Por lo tanto, la compañía eligió acogerse al Capítulo 11, lo cual le permite continuar sus operaciones mientras lleva a cabo una reestructuración financiera destinada a satisfacer las deudas con sus acreedores. Sin embargo, los términos y condiciones de servicio de Celsius Network podrían representar un obstáculo considerable para los clientes que intenten recuperar la totalidad de sus inversiones. Al aceptar estas condiciones, los usuarios conceden a Celsius "todos los derechos y títulos" sobre sus criptoactivos, lo que incluye los "derechos de propiedad" y la autoridad para "pignorar, volver a pignorar, hipotecar, rehipotecar, vender, prestar o transferir, o de cualquier otra forma utilizar" los activos sin limitaciones. Esta disposición convierte a los usuarios en acreedores no garantizados en caso de bancarrota, lo cual es especialmente problemático puesto que, en los procedimientos de quiebra tradicionales, las deudas se valoran en dólares estadounidenses basándose en el valor al momento de la declaración de bancarrota. Esta situación, combinada con la volatilidad inherente del mercado de criptomonedas, podría resultar en pérdidas significativas para los usuarios afectados.

En su comparecencia judicial, Celsius Network informó que el valor de sus activos experimentó una reducción significativa, pasando de 22.100 millones de dólares a tan solo 4.300 millones de dólares en el transcurso del año 2022. Esto refleja una disminución de 17.800 millones de dólares en su valor desde el 30 de marzo de ese mismo año.

Por otro lado, en noviembre de 2022 tuvo lugar la caída de FTX, una de las plataformas de intercambio de criptomonedas más grandes y reconocidas, debido a una combinación de mala gestión, prácticas financieras riesgosas y una crisis de liquidez. Dado que FTX era el emisor de su propio token, el aumento en su valor llevó a que los informes financieros de la empresa mostraran ganancias significativas.

En respuesta, la plataforma de intercambio comenzó a usar este token como colateral para solicitar préstamos, alcanzando una suma de 8 mil millones de dólares estadounidenses, en este caso, a través de Alameda Research, un fondo de comercio de criptomonedas afiliado a FTX y dirigido por Sam Bankman-Fried, cuyo capital total de activos superaba los 14 mil millones de USD. En esencia, la compañía estaba utilizando su propio token para inflar artificialmente sus finanzas, lo cual se reflejaba en sus estados financieros como ganancias generadas a partir de la moneda que ellos mismos emitían.

La crisis se desencadenó cuando un reporte de CoinDesk publicó un balance filtrado de Alameda Research donde se mostraba que gran parte de sus activos estaba compuesta por FTT, el token nativo de FTX, que permitía a los usuarios del exchange recibir beneficios como reducción de comisiones en trading. Esto generó preocupaciones sobre la solidez financiera de Alameda y, por extensión, de FTX. La publicación del reporte llevó a una falta de confianza en FTX, provocando que los usuarios comenzaran a retirar sus fondos masivamente, temiendo por la seguridad de sus activos, incluyendo entre estos a Binance, el exchange más grande a nivel mundial, que anunció que vendería todas sus tenencias en FTT.

Por su parte, FTX no pudo manejar la avalancha de retiros debido a una insuficiencia de liquidez. Informes posteriores sugirieron que FTX había utilizado los depósitos de los clientes para respaldar las operaciones de Alameda Research, una práctica que generó cuestionamientos éticos y legales.

En un intento por salvar la situación, FTX llegó a un acuerdo con Binance, su principal competidor, para una posible adquisición. Binance inicialmente mostró interés en adquirir FTX para ayudar a cubrir el déficit de liquidez, pero descubrió problemas financieros más graves de lo esperado y se retiró del acuerdo, citando preocupaciones sobre la gestión de los fondos de los clientes y posibles investigaciones regulatorias.

La caída drástica de más del 90% en el valor del token FTT desencadenó la liquidación de todas las garantías asociadas a los préstamos de FTX y Alameda Research, lo cual colocó a la plataforma de intercambio en una posición crítica debido a la falta de liquidez necesaria para cumplir con sus obligaciones de pago. Esta situación hizo que FTX suspendiera los retiros de criptomonedas para todos sus usuarios, generando una ola de pánico entre ellos al encontrarse sus fondos bloqueados sin posibilidad de retiro.

Enfrentando una crisis insuperable, FTX se declaró en bancarrota el 11 de noviembre de 2022 mediante la protección del Capítulo 11 de la Ley de Quiebras de los Estados Unidos, a través de la cual se brinda la posibilidad de salvaguardar los activos de la compañía de los reclamos de los acreedores mientras se lleva a cabo el proceso de liquidación. Por su parte, Sam Bankman-Fried renunció como CEO, y John J. Ray III fue nombrado para supervisar el proceso de bancarrota.

El 19 de enero de 2022, la Comisión de Bolsa y Valores de Estados Unidos (SEC) formalizó las acusaciones contra Sam Bankman-Fried (SBF) por delitos de fraude y lavado de dinero. Anteriormente, la SEC había imputado a SBF en relación con el colapso de FTX y por la desaparición de fondos retenidos en su propia empresa durante su declaración de bancarrota.

La quiebra de FTX tuvo un impacto significativo en el mercado global de criptomonedas, erosionando la confianza de los inversores y calificado como "uno de los fraudes más grandes en la historia de Estados Unidos". Este suceso, en el que un proyecto aparentemente exitoso en el mundo de las criptomonedas resultó ser un fraude, ha contribuido significativamente al aumento del escrutinio regulatorio en este sector centrado en posibles violaciones de la ley y mal manejo de los fondos de los clientes.

Ulrich Bindseil, director general de infraestructuras de mercado y pagos, junto con Jürgen Schaaf, consejero sénior en el mismo departamento del Banco Central Europeo, expresaron en el blog de la institución la desconfianza que han generado las criptomonedas entre varios entes reguladores y organismos gubernamentales debido que el uso de criptomonedas en mercados opacos o para la transacción de bienes y servicios ilícitos ha sido notable, contribuyendo al crecimiento de estos mercados al ofrecer un nivel de anonimato elevado, dada la complejidad de rastrear estos activos digitales. Además, se destaca que las criptomonedas carecen de generación de flujos de efectivo comparables a los de los bienes raíces, no ofrecen distribuciones de dividendos al igual que las acciones, no poseen una aplicación productiva similar a las materias primas, ni contribuyen con beneficios sociales equivalentes a los del oro. Por consiguiente, su valorización en el mercado se basa exclusivamente en actividades especulativas.

Finalmente, estos expertos también destacan el considerable impacto ambiental de las criptomonedas, condenando especialmente al sistema de Bitcoin por ser un gran contaminante. Remarcan que, por un lado, el consumo energético de la minería de Bitcoin es desmesurado, comparable al consumo eléctrico anual de países como Austria. Por otro lado, señalan la generación excesiva de residuos electrónicos, indicando que una sola transacción de Bitcoin equivale a la cantidad de hardware desechado de dos smartphones. De manera global, el sistema de Bitcoin produce una cantidad de basura electrónica comparable a todo lo generado por los Países Bajos.

# 4. SITUACIÓN ACTUAL DEL MERCADO DE CRIPTOMONEDAS

Uno de los grandes atractivos de las divisas digitales es la complejidad de rastreo de las transacciones que se realizan con estas. No obstante, los Bancos se encuentran estudiando la posibilidad de lanzar sus propias versiones de monedas digitales. Una limitación importante de las criptomonedas radica en la ausencia de un activo tangible que respalde su valor, lo cual plantea un obstáculo para su evolución puesto que no se consiguen satisfacer de forma simultánea los tres criterios fundamentales: descentralización, rentabilidad en términos de costes y eficacia en la ejecución de transacciones. En consecuencia, los pagos efectuados con estas monedas digitales no son considerados tan eficientes como aquellos realizados con dinero fiduciario.

Durante el año 2023, la Comisión de Bolsa y Valores de Estados Unidos (SEC) ha implementado varias acciones reguladoras en el sector de los criptoactivos. En febrero, el organismo declaró su intención de reforzar las condiciones bajo las cuales plataformas de intercambio como Coinbase y Binance pueden manejar los activos de clientes institucionales. Previamente, las criptomonedas estaban exentas de las directrices aplicables a los custodios cualificados, liberándolas de cumplir con determinadas normativas. Poco antes, la agencia dirigida por Gary Gensler, presidente de la SEC, prohibió la emisión de la moneda estable (*stablecoin*) de Binance (BUSD) y ordenó detener el servicio de *staking* (un mecanismo de minería de criptomonedas) ofrecido por Kraken, otro exchange de criptomonedas. El valor de los criptoactivos ha sido negativamente impactado por el incremento de los tipos de interés, afectando adversamente a las inversiones de alto riesgo. Posteriormente, los diversos escándalos sucedidos han contribuido a una caída en su valorización, resultando en pérdidas multimillonarias en el mercado.

Por otro lado, Binance, la plataforma de intercambio de criptomonedas más grande a nivel mundial, junto a su CEO, Changpeng Zhao (conocido popularmente como CZ), han alcanzado un acuerdo con el Departamento de Justicia de Estados Unidos para admitir responsabilidad en una serie de infracciones tanto civiles como penales. Este acuerdo implica la renuncia de CZ y el pago de una multa, propuesta por el mencionado departamento, que se anticipa ascienda a unos 4.300 millones de dólares.

Como parte del convenio, CZ ha consentido en renunciar a su cargo de director ejecutivo en la compañía y aceptar la culpabilidad por incumplir las normativas de prevención del lavado de activos, en negociaciones que también incluyeron al Departamento del Tesoro. A cambio, el sistema judicial estadounidense permitirá que Binance siga operando dentro del país, poniendo fin a investigaciones sobre delitos que abarcan desde el lavado de dinero y el fraude bancario hasta el incumplimiento de sanciones dirigidas a individuos y países bajo observación, con especial atención en Rusia e Irán.

Respecto a la situación de Terra Luna y su ecosistema asociado había atravesado cambios significativos tras el colapso ocurrido en mayo de 2022. Como respuesta al colapso, la comunidad detrás de Terra propuso y ejecutó un plan de reestructuración que dio origen a una nueva cadena de bloques, conocida como Terra (LUNA), mientras que la cadena original fue renombrada como Terra Classic (LUNC), y la criptomoneda original LUNA pasó a llamarse LUNC. La nueva cadena de bloques se lanzó sin una moneda estable algorítmica, centrándose en lugar de ello en proporcionar una base sólida para futuras aplicaciones descentralizadas y proyectos dentro del ecosistema. Desde entonces, la nueva versión de Terra ha estado trabajando para reconstruir su reputación y establecer un ecosistema sostenible. Sin embargo, la confianza de los inversores y la adopción general han enfrentado desafíos puesto que la situación legal de Do Kwon y las investigaciones en curso por parte de autoridades de varios países, incluyendo Corea del Sur y Estados Unidos, también forman parte de la situación actual del proyecto. Estas investigaciones se centran en las circunstancias que rodearon el colapso de la moneda estable UST y la posible manipulación del mercado o malversación de fondos.

Recientemente, la criptomoneda Terra Classic (LUNC) ha presentado avances significativos en su cotización, observándose el pasado febrero de 2024 un incremento notable en su valor y en el volumen de transacciones. Específicamente, el 4 de febrero, el precio de Terra Classic (LUNC) dio un salto importante, acompañado de un incremento del 700% en el volumen de transacciones. A pesar de los desafíos previos de LUNC, estos signos positivos podrían indicar un cambio de tendencia. Asimismo, existe una expectativa creciente de que el precio de Terra Classic (LUNC) pueda llegar al dólar durante el año en curso. El propósito de Terra Classic (LUNC) es recuperar su valor original ligado al USTC y al dólar estadounidense, mediante la quema de billones de tokens LUNC generados durante su colapso. Aunque los recientes desarrollos son alentadores, el precio de Terra Classic (LUNC) ha empezado a evidenciar una corrección negativa. Además, el mercado muestra una falta de dirección definida, haciéndolo susceptible a fluctuaciones de precio imprevistas. En un escenario bajista, si LUNC no consigue sostenerse por encima del nivel de soporte de 0.00010104 dólares, se podría desencadenar una tendencia a la baja, potencialmente cayendo más allá de los 0.00009564 dólares y 0.00009472 dólares.

Respecto a Celsius Network, la compañía recientemente ha anunciado la venta de 206.300 Ethereum, lo cual equivale a aproximadamente 470 millones de dólares. Esta transacción representa un paso crucial para la compañía en su esfuerzo por restaurar su solidez financiera, afrontar los pagos adeudados a sus acreedores, manejar los costes derivados de su proceso de reestructuración y satisfacer los compromisos adquiridos en el marco de su procedimiento bajo el Capítulo 11.

En este contexto, Alex Mashinsky, ex director ejecutivo de la firma, está enfrentando complicaciones legales, incluido su arresto en julio de 2023 por cargos de fraude relacionados con alegaciones de haber difundido información falsa acerca de la solvencia financiera de Celsius Network, situación que ha resultado en la inmovilización judicial de sus activos. Como parte de la estrategia de reestructuración, Celsius Network ha creado MiningCo, una nueva entidad que ofrece participación a los acreedores, mostrando así su compromiso de incluir a las partes interesadas en su proceso de reorganización. Paralelamente, la compañía está elaborando estrategias para NewCo, una entidad proyectada para enfocarse en actividades de *staking* y minería, con el objetivo de reforzar las operaciones y tácticas comerciales de la compañía. El 31 de enero de 2024, Celsius Network anunció el comienzo de la entrega de 3 mil millones de dólares en criptomonedas y efectivo a sus acreedores, señalando así su salida oficial del Capítulo 11 de quiebras, evento que ocurría 18 meses después de que la plataforma suspendiera las retiradas de fondos por parte de los usuarios.

En el marco del plan de reestructuración aprobado, se ha asignado una porción de los 3 mil millones de dólares a la fundación de Ionic Digital, una naciente entidad dedicada a la minería de bitcoin, la cual será transferida a los acreedores. Estos obtendrán acciones ordinarias de la entidad, las cuales se anticipa que serán listadas en el mercado de valores una vez se consigan las autorizaciones requeridas. La supervisión de las actividades mineras de Ionic recaerá en Hut 8, una operadora minera establecida en Miami, mediante un contrato de gestión que se extenderá por cuatro años. Este movimiento implica que Celsius Network planea una retirada ordenada del mercado, procediendo al cierre progresivo de sus aplicaciones tanto en versiones web como móviles.

En cuanto a la desaparecida bolsa de criptomonedas FTX, ésta ha aclarado que su estrategia de reestructuración no contempla una reactivación del negocio, sino que se enfoca en la completa compensación a sus clientes. Durante una sesión judicial el 31 de enero de 2024, el abogado representante de FTX, Andy Dietderich, subrayó que, pese a los esfuerzos realizados, no existen intenciones de reanudar las operaciones de FTX.

Previo a esta declaración, numerosos usuarios de FTX solicitaron al Tribunal de Quiebras de Delaware la prohibición a la plataforma colapsada de evaluar sus depósitos de criptomoneda basándose en los precios del año 2022 argumentando que tal método les restringía la posibilidad de aprovechar el reciente ascenso en los valores del mercado cripto. El 11 de noviembre de 2022, fecha en que FTX declaró su bancarrota, el precio de Bitcoin apenas superaba los 17.000 dólares. Actualmente, su valor se ubica cerca de los 43.600 dólares aproxidamente, una tendencia al alza que se observa en varias criptomonedas presentes en el mercado. Esto implica que parte de los activos en poder de FTX han experimentado un incremento en su valor, aunque las deudas se liquidarán con los precios anteriores.

Esta apreciación facilitará la cancelación de un mayor número de obligaciones que si los reembolsos se efectuaran con base en las cotizaciones actuales. Por consiguiente, si un usuario tenía 0,25 BTC en su cuenta del exchange, recibirá 4.250 dólares en lugar de los 10.900 dólares que representarían actualmente.

Respecto otras criptomonedas como Tether, dicho token es cada vez más favorecido por los estafadores y blanqueadores de dinero que operan en el sudeste asiático, tal y como advierte la ONU. En su informe se destaca que las plataformas de apuestas en línea, principalmente aquellas que operan de manera ilegal, se han convertido en importantes canales para el blanqueo de capitales mediante criptomonedas, siendo Tether uno de los tokens más utilizados por los blanqueadores. A pesar de los esfuerzos por controlar el uso de activos digitales, los grupos delictivos continúan prefiriendo Tether como una herramienta efectiva para la transferencia de fondos ilícitos lo cual ha llevado a que algunos casinos en línea se especialicen en la gestión de dicho token. Según el informe de la ONU, en los últimos años, las autoridades han logrado desmantelar diversas redes de blanqueo que utilizaban Tether, incluyendo una operación en Singapur que permitió recuperar 737 millones de dólares entre efectivo y criptomonedas en agosto del año pasado. Además, en noviembre, tras una investigación en colaboración con autoridades de Estados Unidos y la plataforma de intercambio de criptomonedas OKX, se logró que Tether congelara 225 millones de dólares en tokens vinculados a redes de tráfico de personas en el sudeste asiático.

En el contexto actual de España, se ha observado que un número significativo de individuos, superando los 150.000, han optado por registrar sus datos biométricos oculares a cambio de una recompensa monetaria cifrada en tokens, con un valor aproximado de 100 euros. Este grupo demográfico está compuesto mayoritariamente por jóvenes y personas de bajos recursos económicos. Este notable fenómeno tiene sus orígenes en las iniciativas lideradas por Sam Altman, presidente de OpenAI, y Alex Blania, presidente de Tools for Humanity. Ambos están al frente de Worldcoin, un proyecto que ha venido desarrollándose discretamente, mientras la atención pública se centraba en otros desarrollos tecnológicos como ChatGPT. La ambición de Worldcoin es implementar un sistema de identificación biométrica universal mediante el escaneo del iris de la población global, con el objetivo a largo plazo de abarcar a unos 2.000 millones de personas, lo que equivaldría a aproximadamente un cuarto de la población mundial. Paralelamente, se aspira a establecer una base económica que permita la distribución de una Renta Básica Universal financiada por los avances en Inteligencia Artificial, ideada para redistribuir los beneficios generados por esta tecnología y mitigar los impactos negativos en el empleo, aunque actualmente este aspecto del proyecto aún se encuentra en una fase conceptual.

Para asegurar una asignación justa y evitar registros duplicados, los promotores del proyecto han optado por la utilización de escáneres biométricos del iris. Este procedimiento se lleva a cabo mediante un dispositivo esférico denominado "Orb", el cual convierte la imagen capturada del iris en una secuencia numérica cifrada (hash), garantizando la imposibilidad de reconstruir la imagen original a partir de esta secuencia, incluso en caso de compromiso de la misma.

Este sistema encriptado permite la verificación de identidades sin almacenar datos biométricos directos ni permitir su rastreo o acceso por terceros. Si el usuario no ha sido previamente registrado, su información se incorpora a la base de datos y al blockchain de la compañía. Como incentivo, Worldcoin ofrece recompensas que pueden incluir dinero en efectivo o tokens de su propia criptomoneda, Worldcoin (WLD).

En lo que respecta a la privacidad y el manejo de datos, Worldcoin asegura eliminar las imágenes capturadas y remite a sus políticas de privacidad publicadas en su sitio web. Sin embargo, también admiten la posibilidad de compartir información con terceras partes, como proveedores de servicios tecnológicos y entidades bancarias, e incluso con gobiernos para cumplir con obligaciones legales.

Desde el ámbito académico, Carissa Véliz, profesora de Filosofía en la Universidad de Oxford y autora de importantes obras sobre la privacidad, enfatiza la importancia del anonimato para la democracia y advierte sobre los riesgos de un sistema global de identificación para las libertades individuales. Asimismo, investigaciones y reportajes han expuesto fallos técnicos y prácticas cuestionables en la implementación del proyecto, incluyendo duplicidades en los registros y estrategias de marketing engañosas en varios países como Indonesia, Kenia, Sudán o Ghana.

En el territorio español, actualmente se están investigando varias denuncias contra Worldcoin, interpuestas en Madrid y Cataluña por la Agencia Española de Protección de Datos (AEPD). La Federación de Consumidores y Usuarios (CECU) ha emitido advertencias sobre los peligros de compartir datos biométricos, señalando el alto grado de precisión del escaneo del iris y el potencial riesgo para la privacidad de los usuarios.

En la situación financiera actual de Estados Unidos, la Comisión de Bolsa y Valores (SEC) ha concedido su aprobación formal para el estreno del primer fondo cotizado en bolsa (ETF) de Bitcoin al contado que será regulado dentro del territorio nacional, marcando un hito significativo en el terreno de la normativa financiera. Este acontecimiento sucede tras la confusión ocasionada por un anuncio falso emitido a través de la cuenta oficial de Twitter (X) de la SEC, que previamente había generado considerable agitación en los mercados financieros. El 10 de enero de 2024, la SEC concedió su aprobación a las solicitudes 19b-4 presentadas por entidades tales como ARK 21Shares, Invesco Galaxy, VanEck, WisdomTree, Fidelity y Franklin Templeton, facilitando así los ajustes regulatorios requeridos para la cotización y el comercio de ETFs de Bitcoin al contado.

Los ETFs son fondos cotizados en bolsa que constituyen vehículos de inversión que buscan replicar el desempeño de un activo de referencia, siendo Bitcoin el activo subyacente en este contexto. Estos fondos ofrecen a los inversores la posibilidad de incursionar en el mercado de criptomonedas sin la necesidad de adquirir, custodiar o gestionar los activos digitales de manera directa.

En su lugar, los interesados pueden comprar participaciones del fondo, las cuales se negocian en el mercado de valores al igual que las acciones tradicionales. Este enfoque posibilita que Bitcoin se convierta en el activo subyacente del ETF, lo que podría incidir positivamente en el incremento de la demanda, valorización y adopción general de la criptomoneda.

En palabras de Enrique Palacios Rojo, miembro del Comité de la Autoridad Bancaria Europea (EBA), esta medida habilitará a asesores financieros y gestores de fondos en los Estados Unidos a ofrecer Bitcoin como una opción de inversión, potenciará las operaciones extrabursátiles y mejorará los resultados financieros de los servicios de custodia. Esto se debe a que son las entidades gestoras quienes adquieren los criptoactivos que posteriormente son custodiados, para su mejor diversificación de los riesgos asociados. Javier García de la Torre, director de Binance para España y Portugal, considera que los ETFs de Bitcoin al contado mejorarán el acceso al mercado de las criptodivisas, atrayendo un mayor número de inversores y aumentando la liquidez, lo cual conferirá mayor credibilidad al sector de los activos digitales. No obstante, Albert Salvany, socio fundador de Funding Fast, anticipa una intensificación de la competencia en términos de comisiones entre los proveedores de ETFs y otros intermediarios del mercado de criptoactivos.

La aprobación de estos ETFs acarrea consecuencias significativas, como el aumento de la accesibilidad para una amplia gama de inversionistas, tanto institucionales como minoristas, y la posibilidad de que aquellos fondos sujetos a restricciones regulatorias o políticas internas que les impedían invertir directamente en criptomonedas ahora puedan hacerlo. Se espera que esto contribuya a una mayor liquidez en el mercado de Bitcoin, fomentando un incremento en el volumen de negociación y una posible reducción en la volatilidad de los precios. Asimismo, se anticipa que el lanzamiento de estos ETFs pueda tener un impacto positivo en el precio del Bitcoin y fomentar la confianza entre nuevos segmentos de inversores, promoviendo una adopción financiera más amplia de las criptomonedas. No obstante, la implementación de los ETFs de Bitcoin al contado no está exenta de riesgos y desafíos potenciales, incluida la posibilidad de una supervisión regulatoria más rigurosa que podría obstaculizar el desarrollo del mercado, así como la incertidumbre legal en ciertos países que podría restringir el crecimiento del mercado de criptoactivos.

En conclusión, mientras que el creciente interés por parte de las instituciones financieras en el Bitcoin constituye un factor que podría impulsar la demanda y el valor de esta criptomoneda, es importante considerar que existen diversos factores, incluidas las consideraciones regulatorias y la incertidumbre legal, que podrían influir negativamente o generar incertidumbre respecto al precio del Bitcoin en el futuro.

# 5. RELACIÓN Y COMPARATIVA CON BURBUJAS INVERSORAS

La historia financiera reciente está marcada por episodios significativos de inestabilidad, entre los que destacan la burbuja de las empresas *punto com* a finales de los años 90 y principios de los 2000, la crisis de las hipotecas *subprime* en Estados Unidos en 2007, y la burbuja inmobiliaria que desencadenó la crisis financiera en España entre 2010 y 2012. Aunque cada una de estas crisis tiene características propias, derivadas del contexto económico, social y tecnológico en el que se desarrollaron, comparten similitudes notables con la evolución y comportamiento del mercado de las criptomonedas los cuales subrayan la importancia de la regulación, la percepción de valor y el impacto de la especulación en la formación y estallido de burbujas financieras.

Respecto a la burbuja de las empresas *punto com*, ésta fue impulsada por el entusiasmo excesivo en torno a las posibilidades de internet. Se caracterizó por una especulación desenfrenada que llevó a valoraciones infladas de empresas tecnológicas, muchas de las cuales tenían modelos de negocio insostenibles o incluso inexistentes. La crisis *subprime*, por otro lado, fue el resultado de prácticas de préstamo irresponsables y la creación de productos financieros complejos que ocultaban el riesgo real de las hipotecas de baja calidad; mientras que la crisis inmobiliaria española compartió este último aspecto, siendo alimentada por un acceso fácil al crédito y una especulación intensa en el sector inmobiliario, lo que llevó a una sobrevaloración masiva de los activos inmobiliarios.

La relación de dichas crisis con el mercado de las criptomonedas puede observarse en varios aspectos. Primero, la especulación ha sido un motor común en todas ellas, alimentada por expectativas de rápidos retornos y una adopción masiva por parte de inversores sin una comprensión adecuada de los activos subyacentes o los riesgos involucrados. En el caso de las criptomonedas, la volatilidad y las enormes ganancias potenciales han atraído tanto a inversores experimentados como a inversores poco informados, muchos de los cuales no están preparados para las fluctuaciones extremas del mercado. En cada caso, la promesa de una nueva era económica o tecnológica contribuyó a desvincular los precios de los activos de sus fundamentos económicos reales, llevando eventualmente a correcciones de mercado y crisis financieras. Por otro lado, la importancia de una regulación adecuada y proactiva es evidente en la prevención y mitigación del impacto de estas burbujas, puesto que la falta de esta o la regulación inadecuada ha sido un factor crítico en la expansión de estas crisis. Mientras que el sector de las criptomonedas ha operado en gran medida fuera de los marcos regulatorios tradicionales, los episodios anteriores han demostrado la necesidad de supervisión para proteger a los inversores, mantener la estabilidad del mercado y evitar consecuencias económicas negativas más amplias.

En tercer lugar, la innovación tecnológica ha jugado un papel central en la creación de estas burbujas. Así como la revolución de internet y el desarrollo de instrumentos financieros complejos facilitaron las burbujas *punto com* y *subprime*, la tecnología blockchain y las criptomonedas representan una nueva frontera que a menudo ha eclipsado las evaluaciones racionales de su valor real y su sostenibilidad a largo plazo.

En conclusión, el estudio comparativo de las burbujas financieras asociadas a las criptomonedas con otras burbujas históricas subraya la complejidad de los mercados financieros y la necesidad constante de vigilancia, tanto por parte de los reguladores como de los inversores, para discernir entre la innovación genuina y la especulación desenfrenada. La comprensión de estas dinámicas es crucial para el desarrollo de estrategias que fomenten la estabilidad financiera y protejan los intereses de los participantes del mercado en el largo plazo, por lo que la historia sugiere que la prudencia, la educación financiera, una comprensión profunda de los activos, una regulación equilibrada y una evaluación cuidadosa de los riesgos son esenciales para navegar en estos mercados volátiles y evitar así las consecuencias devastadoras que pueden seguir al estallido de una burbuja financiera.

# 6. CONCLUSIONES

En la elaboración de este trabajo de final de grado, se ha explorado exhaustivamente la economía de las criptomonedas, desde su naturaleza deflacionaria y métodos de adquisición hasta su utilidad como medio de intercambio. Se ha profundizado en las características y diferencias entre Bitcoin y Ethereum, dos de las criptomonedas más prominentes, y se han examinado los complejos aspectos legales y regulatorios que las envuelven, así como los riesgos y desafíos inherentes a este innovador sector financiero. La problemática de las plataformas exchange, esencial para la operativa de las criptomonedas, también ha sido analizada, destacando los riesgos de seguridad y la necesidad de una regulación más coherente y global. La situación actual del mercado de criptomonedas, caracterizada por su volatilidad y crecimiento exponencial, refleja tanto el enorme potencial de esta tecnología como los desafíos significativos que enfrenta. La comparativa con burbujas financieras históricas ha permitido identificar similitudes, como la especulación y el exceso de optimismo.

Una de las conclusiones primordiales de este análisis es que, a pesar de las diferencias contextuales y operativas entre las criptomonedas y las burbujas financieras históricas examinadas, existen patrones comunes que sugieren una tendencia inherente a la especulación excesiva, la innovación tecnológica disruptiva y las lagunas regulatorias. Estos factores ponen en evidencia la importancia de una comprensión profunda y crítica de los activos financieros emergentes y la necesidad de un marco regulatorio adaptativo y proactivo. Asimismo, este trabajo ha destacado la importancia de la educación financiera y tecnológica como herramientas esenciales para mitigar los riesgos asociados a la inversión en activos altamente volátiles y especulativos como las criptomonedas. La promoción de una cultura de inversión informada y responsable puede desempeñar un papel crucial en la prevención de las consecuencias negativas derivadas de las dinámicas de burbuja financiera.

Finalmente, se plantea la necesidad de un diálogo continuo entre desarrolladores tecnológicos, reguladores financieros, inversores y académicos para explorar las potencialidades de las criptomonedas como instrumentos financieros innovadores, al tiempo que se asegura la protección de los inversores y la estabilidad del sistema financiero global. Este equilibrio será esencial para aprovechar los beneficios de la innovación tecnológica en el sector financiero, minimizando al mismo tiempo los riesgos de inestabilidad y pérdida financiera.

En resumen, el estudio de la problemática de las criptomonedas y su comparativa con episodios históricos de burbujas financieras revela la complejidad de los mercados financieros modernos y subraya la importancia de abordar estos desafíos con un enfoque multidisciplinario e integrador, que combine la prudencia regulatoria con la innovación y la educación financiera.

# 7. BIBLIOGRAFÍA


- Agencia Estatal. (2016, 12 de julio). *A-2021-11473 Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal* . Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2021-11473&p=20211012&tn=2

- Agencia Estatal. (2019, 9 de marzo). *Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio.* Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2006-20764&p=20211109&tn=1#dadecimotercera

- Agencia Estatal. (2022, 17 de diciembre). *A-2003-23186 Ley 58/2003, de 17 de diciembre, General Tributaria.* Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2003-23186&p=20210710&tn=1#dadecimoctava

- Agencia Estatal. (2023, 31 de mayo). *Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937*. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80808

- Ambrissi, P. (2024, 21 de febrero). *Terra Classic (LUNC) aumentó en su precio y volumen de operaciones*. Cointelegraph. https://es.cointelegraph.com/news/terra-classic-lunc-increased-price-and-trading-volume

- Antonopoulos, A. M. (2014). *Mastering Bitcoin*. O'Reilly. https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf

- Arjona Brescolí, A. (2013). *La contabilidad triangular o de partida triple*.

- Arroyo, M., & Clementín, F. (2022, 18 de noviembre). *10 claves para entender qué pasó con FTX*. CriptoNoticias. https://www.criptonoticias.com/negocios/10-claves-entender-que-paso-ftx/

- Ayala, G. (2018, 1 de noviembre). *¿Qué es la deflación en Bitcoin?* Bit2Me Academy. https://academy.bit2me.com/que-es-deflacion-bitcoin/

- Bandovic Raskovic, N. (2021/2022). *La auditoría de las criptomonedas: el Bitcoin. Un estudio en España, Unión Europea y EE.UU.* UPV. https://riunet.upv.es/bitstream/handle/10251/188715/Bandovic%20-%20La%20auditoria%20de%20las%20criptomonedas%20el%20Bitcoin%20Un%20estudio%20en%20Espana%20Union%20Europea%20y%20EEUU.pdf?sequence=1&isAllowed=y

- Barroso, P. (2022, 30 de diciembre). *Apocalipsis 'cripto': Las 20 principales criptomonedas caen más del 50%.* Economia 3. https://economia3.com/2022/12/26/514039-apocalipsis-cripto-las-20-principales-criptomonedas-caen-mas-del-50-este-ano/

- Bhosale, J., & Mavale, S. (2018). Volatility of select crypto-currencies. A comparision of Bitcoin, Etherreum and Litecoin. Annual Research Journal of SCMS, 6, 132-141.

- Blockchain.com. (n.d.). *Charts - Total Circulating Bitcoin.* Blockchain.com. https://www.blockchain.com/explorer/charts/total-bitcoins

- Carriere, E. (2022, 24 de mayo). *¿Por qué se colapsó Terra LUNA y UST? ¿cómo ocurrió?* Coinmotion. https://coinmotion.com/es/causas-colapso-terra-luna-ust/

- Centro Europeo del Consumidor España. (2023, 8 de mayo). *Centro Europeo del Consumidor en España - Ministerio de Consumo - El Parlamento Europeo aprueba la primera regulación sobre criptoactivos con la que se protegerá mejor al consumidor.* Centro Europeo del Consumidor en España. https://cec.consumo.gob.es/CEC/comunicacion/noticias/2023/NI_Regulacion_Criptomonedas_08_05_2023.htm

- Chipolina, S. (2024, 14 de enero). Tether crypto token increasingly favoured by money launderers, UN warns. Financial Times. https://www.ft.com/content/78c6ea20-5e9d-40ba-867f-1e0431ebb710

- Civieta, Ó. F. (2023, 14 de mayo). *Cuál es el futuro de las criptomonedas tras el criptoinvierno.* Business Insider España. https://www.businessinsider.es/cual-futuro-criptomonedas-criptoinvierno-1243170

- Coin Edition. (2023, 24 de agosto). *Celsius presenta plan de pago para clientes tras aprobación judicial.* Coin Edition. https://coinedition.com/es/celsius-presenta-plan-de-pago-para-clientes-tras-aprobacion-judicial/

- Comunidad de Madrid. (n.d.). *Comprar con criptomonedas. ¿A qué nos enfrentamos? | Comunidad de Madrid.* Comunidad de Madrid. https://www.comunidad.madrid/servicios/consumo/comprar-criptomonedas-nos-enfrentamos

- Decker, C., & Wattenhofer, R. (n.d.). *Bitcoin Transaction Malleability and MtGox*. M. Kutylowski and J. Vaidya (Eds.): ESORICS 2014, Part II, LNCS 8713, pp. 313–326, 2014.

- elEconomista.es & Bloomberg. (2023, 21 de noviembre). *Binance pagará 4.300 millones a la Justicia de EEUU por blanqueo de capitales y su CEO dimite*. elEconomista.es. https://www.eleconomista.es/mercados-cotizaciones/noticias/12550278/11/23/el-ceo-de-binance-cz-se-declara-culpable-de-blanqueo-de-capitales-en-eeuu-y-acepta-su-dimision.html

- Erard, G. (2024, 31 de enero). FTX devolverá los fondos de todos sus clientes, pero tiene truco. Hipertextual. https://hipertextual.com/2024/01/ftx-promete-devolver-fondos-clientes

- Escribano, M. (2023, 13 de agosto). Nadie sabe por qué el creador de ChatGPT quiere tus ojos, pero hay motivos para preocuparte. El Confidencial. https://www.elconfidencial.com/tecnologia/2023-08-13/worldcoin-sam-altman-iris-biometria-inteligencia-artificial_3715840/

- Fernández, R. (2023, 14 de marzo). *Bitcoin: cotización en XBT/USD 2019-2023*. Statista. https://es.statista.com/estadisticas/636506/cotizacion-de-bitcoins-en-dolares-estadounidenses/

- Frota Decourt, R., Chohan, U. W., & Perugini, M. L. (2017). *Bitcoin returns and the Weekday Effect*. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435176

- FXMAG. (2023, 20 de enero). *JP Morgan cree que las criptomonedas son un fraude, mientras la SEC acusa a Sam Bankman por defraudar a los inversores de FTX. Precio Bitcoin DÓLAR (BTCUSD) hoy Por FXMAG Spain*. Investing.com. https://es.investing.com/news/economy/jp-morgan-cree-que-las-criptomonedas-son-un-fraude-mientras-la-sec-acusa-a-sam-bankman-por-defraudar-a-los-inversores-de-ftx-precio-bitcoin-dlar-btcusd-hoy-2346848

- García, L. (2022, abril). *ANÁLISIS CAUSAL DEL EFECTO CRISIS EN LAS CRIPTOMONEDAS*. Universidad Pontificia de Comillas. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/57262/TFG-Garcia%20Taboadela%2C%20Laura.pdf?sequence=2&isAllowed=y

- García, L. M. (2023, 25 de abril). *Uno de los grandes defensores de bitcoin: "Las criptomonedas están muertas en Estados Unidos"*. elEconomista.es. https://www.eleconomista.es/mercados-cotizaciones/noticias/12244895/04/23/uno-de-los-grandes-defensores-de-bitcoin-las-criptomonedas-estan-muertas-en-estados-unidos.html

- Godoy, G. (2023, 15 de julio). *¿Qué podemos aprender de la caída de Celsius?* Cointelegraph. https://es.cointelegraph.com/news/what-can-we-learn-from-the-fall-of-celsius

- Godoy, G. (2024, 5 de febrero). Bitcoin y los ETF: ¿Qué pasa si los reguladores frenan el entusiasmo? Cointelegraph. https://es.cointelegraph.com/news/bitcoin-and-etfs-what-happens-if-regulators-curb-the-enthusiasm

- González Medina, R. (2019, junio). *Análisis y evolución de una criptomoneda: el Bitcoin*. Depósito de Investigación Universidad de Sevilla. https://idus.us.es/handle/11441/88970

- Huang, K. (2022, 14 de noviembre). ¿Qué pasó con FTX? Esto es lo que tienes que saber (Published 2022). *The New York Times*. https://www.nytimes.com/es/2022/11/14/espanol/ftx-criptomonedas-que-paso.html

- Jiménez, M. (2024, 10 de enero). La SEC anuncia en falso la aprobación de una inversión en bitcoin tras el pirateo de su cuenta en X. EL PAÍS. https://elpais.com/economia/2024-01-10/la-sec-anuncia-en-falso-la-aprobacion-de-una-inversion-en-bitcoin-tras-el-pirateo-de-su-cuenta-en-x.html

- Jiménez Romero, K. (2024, 24 de febrero). España evalúa denuncias contra Worldcoin. Cointelegraph. https://es.cointelegraph.com/news/spain-evaluates-complaints-against-worldcoin

- Kethineni, S., Cao, Y., & Dodge, C. (2017, mayo). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, 18. 10.1007/s12103-017-9394-6

- Maldonado, J. (2022, 9 de agosto). *Análisis: ¿Qué pasó en Celsius Network?* Bit2Me News. https://news.bit2me.com/analisis-que-paso-en-celsius-network/

- Mendoza Tello, J. C., Mora Mora, H., & Pujol López, F. A. (n.d.). *Innovación disruptiva de las criptomonedas para la sociedad y el comercio electrónico*. RUA. https://rua.ua.es/dspace/bitstream/10045/95528/1/tesis_julio_mendoza.pdf

- Millán, V. (2024, 23 de febrero). Conseguir una renta básica universal gracias a tu iris: el supuesto objetivo final de Sam Altman con Worldcoin. elEconomista.es. https://www.eleconomista.es/tecnologia/noticias/12689623/02/24/conseguir-una-renta-basica-universal-el-supuesto-objetivo-final-de-sam-altman-con-worldcoin.html

- Mitchelhill, T. (2024, 10 de enero). *ACTUALIZADO: ETF de Bitcoin al contado recibe aprobación oficial de la SEC*. Cointelegraph. https://es.cointelegraph.com/news/sec-spot-bitcoin-etf-approvals

- Monchau, C. (2022, 16 de noviembre). *FTX: one scandal too many for cryptos?* Syz Blog. https://blog.syzgroup.com/crypto-corner/ftx-one-scandal-too-many-for-cryptos

- Mori Sanchez, D. A. (2021, febrero). *Las criptomonedas como aportes societarios para la constitución de una sociedad o el aumento de capital de esta, en el marco de la ley n° 26887 – ley general de sociedades*. Universidad nacional de Cajamarca. https://repositorio.unc.edu.pe/bitstream/handle/20.500.14074/4027/Deyvih%20Alexander%20Mori%20Sanchez.pdf?sequence=5&isAllowed=y

- Myconomy. (2024, 8 de enero). Celsius Network en quiebra y venta de Ethereum – myconomy. Myconomy. https://myconomy.intereconomia.com/noticias/celsius-network-en-quiebra-y-venta-de-ethereum-20240108-0915/

- Myconomy. (2024, 1 de febrero). Celsius Network distribuye criptomonedas tras salir de bancarrota. Myconomy. https://myconomy.intereconomia.com/noticias/celsius-network-distribuye-3-mil-millones-de-dolares-tras-salir-del-capitulo-11-de-bancarrotas-20240201-1014/

- Narain, A., & Moretti, M. (2022, septiembre). *Regulación de los Criptoactivos*. International Monetary Fund. https://www.imf.org/es/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti

- Newsroom Infobae. (2023, 28 de agosto). *¿Cómo se han comportado las criptomonedas hoy? Análisis de su volatilidad y tendencias*. Infobae. https://www.infobae.com/noticias/2023/08/28/como-se-han-comportado-las-criptomonedas-hoy-analisis-de-su-volatilidad-y-tendencias/

- Nieto Giménez-Montesinos, M.A y Hernáez Molera, J. (2019). Monedas Virtuales y Locales: Las Paramonedas, ¿Nuevas formas de Dinero? Revista de Estabilidad Financiera, Banco de España.

- Nieves, V. (2022, 30 de noviembre). *El BCE asegura que el bitcoin está condenado a caer en la irrelevancia: "Su estabilización es un último suspiro"*. elEconomista.es. https://www.eleconomista.es/mercados-cotizaciones/noticias/12063034/11/22/El-BCE-asegura-que-el-bitcoin-esta-condenado-a-caer-en-la-irrelevancia-Su-estabilizacion-es-un-ultimo-suspiro.html

- Nwaokocha, A. (2024, 4 de febrero). *Relanzamiento de FTX genera alarmas sobre beneficios del equipo legal*. Cointelegraph. https://es.cointelegraph.com/news/ftx-scrapped-relaunch-raises-alarm-on-legal-team-profits

- Parlamento Europeo. (2019, 9 de marzo). *POSICIÓN DEL PARLAMENTO EUROPEO*. Parlamento Europeo. https://www.europarl.europa.eu/doceo/document/TC1-COD-2020-0359_ES.pdf

- Parlamento Europeo. (2022, 1 de abril). *Noticias*. Peligros de las criptomonedas y beneficios de la nueva legislación de la UE | Noticias | Parlamento Europeo. https://www.europarl.europa.eu/news/es/headlines/economy/20220324STO26154/peligros-de-las-criptomonedas-y-beneficios-de-la-nueva-legislacion-de-la-ue

- Parlamento Europeo. (2022, 5 de octubre). *PROVISIONAL AGREEMENT RESULTING FROM INTERINSTITUTIONAL NEGOTIATIONS*. European Parliament. https://www.europarl.europa.eu/RegData/commissions/econ/inag/2022/10-05/CJ12_AG(2022)737215_EN.pdf

- Parlamento Europeo. (2023, 20 de abril). *Luz verde del Parlamento a la primera regulación europea sobre criptoactivos*. Luz verde del Parlamento a la primera regulación europea sobre criptoactivos | Noticias | Parlamento Europeo. https://www.europarl.europa.eu/news/es/press-room/20230414IPR80133/luz-verde-del-parlamento-a-la-primera-regulacion-europea-sobre-criptoactivos

- Parlamento Europeo. (2023, 20 de abril). *POSICIÓN DEL PARLAMENTO EUROPEO*. PARLAMENTO EUROPEO. https://www.europarl.europa.eu/doceo/document/TC1-COD-2020-0265_ES.pdf

- Preukschat, A. (2017). *Blockchain: la revolución industrial de internet*. Grupo Planeta. https://www.academia.edu/36701339/Blockchain_La_revoluci%C3%B3n_industrial_de_internet_Alexander_Preukschat

- PUYOD, S. (2019-2020). *El uso en el mercado económico de los sistemas de criptodivisas*. Trabajo Fin de Grado. https://zaguan.unizar.es/record/90092/files/TAZ-TFG-2020-291.pdf

- Rizzo, P. (2014, 4 de marzo). Bitcoin Bank Flexcoin to Close After $600k Bitcoin Theft. CoinDesk. https://www.coindesk.com/markets/2014/03/04/bitcoin-bank-flexcoin-to-close-after-600k-bitcoin-theft/

- Rodríguez, Ó. (2024, 10 de enero). La SEC dice sí a los ETF de bitcoins: cuatro implicaciones de su aprobación. FundsPeople. https://fundspeople.com/es/la-sec-dice-si-a-los-etf-de-bitcoins-cuatro-implicaciones-de-su-aprobacion/

- Salamanca Peña, D. A., & Suárez Arciniegas, Á. M. (2018, mayo). *Problemas de agencia y teoría de la firma en la financiación mediante ofertas iniciales de criptomonedas*. Universidad de Los Andes. https://repositorio.uniandes.edu.co/bitstream/handle/1992/40199/u807958.pdf?sequence=1&isAllowed=y

- Secretaría de estado de hacienda. Dirección general de tributos. (2018, 11 de junio). *Consultas de la D.G. Tributos*. Consultas de la D.G. Tributos: Buscador. https://petete.tributos.hacienda.gob.es/consultas/?num_consulta=V2679-21&ct=t(EMAIL_CAMPAIGN_1_31_2022_11_26_AR/2022/013)

- Secretaría de estado de hacienda. Dirección general de tributos. (2015, 30 de marzo). *Consultas de la D.G. Tributos*. Consultas de la D.G. Tributos: Buscador. https://petete.tributos.hacienda.gob.es/consultas/

- Tristán Rodríguez, P., Guevara Segarra, M. F., & Cortez Alejandro, K. A. (2019, 31 de julio). *Análisis comparativo entre criptomonedas y el dinero fiduciario*. Universidad Autónoma de Nuevo León. http://www.web.facpya.uanl.mx/vinculategica/vinculategica_5/8%20TRISTAN_GUEVARA_CORTEZ.pdf

- Vásquez-Leiva, M. (2014). Bitcoin: ¿Moneda o burbuja? *Revista Chilena de Economía y Sociedad*, *8*, 54-56.

- Velasco, D., & Fernández, A. (2022, 14 de mayo). Colapso en el mundo de las criptodivisas: Luna deja de orbitar Terra. *El Diario*. https://www.eldiario.es/economia/colapso-mundo-criptodivisas-luna-deja-orbitar-terra_1_8992111.html

# ANEXO I. RELACIÓN DEL TRABAJO CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE DE LA AGENDA 2030

## Anexo al Trabajo de Fin de Grado y Trabajo de Fin de Máster: Relación del trabajo con los Objetivos de Desarrollo Sostenible de la agenda 2030.

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

| Objetivos de Desarrollo Sostenibles | Alto | Medio | Bajo | No Procede |
|---|---|---|---|---|
| ODS 1. **Fin de la pobreza.** | | | | X |
| ODS 2. **Hambre cero.** | | | | X |
| ODS 3. **Salud y bienestar.** | | | | X |
| ODS 4. **Educación de calidad.** | X | | | |
| ODS 5. **Igualdad de género.** | | | | X |
| ODS 6. **Agua limpia y saneamiento.** | | | | X |
| ODS 7. **Energía asequible y no contaminante.** | | X | | |
| ODS 8. **Trabajo decente y crecimiento económico.** | X | | | |
| ODS 9. **Industria, innovación e infraestructuras.** | | | X | |
| ODS 10. **Reducción de las desigualdades**. | | | X | |
| ODS 11. **Ciudades y comunidades sostenibles**. | | | X | |
| ODS 12. **Producción y consumo responsables.** | X | | | |
| ODS 13. **Acción por el clima.** | X | | | |
| ODS 14. **Vida submarina.** | | | | X |
| ODS 15. **Vida de ecosistemas terrestres.** | | | | X |
| ODS 16. **Paz, justicia e instituciones sólidas.** | X | | | |
| ODS 17. **Alianzas para lograr objetivos.** | X | | | |

Descripción de la alineación del TFG/TFM con los ODS con un grado de relación más alto.

El objeto de estudio de este trabajo intersecta con múltiples Objetivos de Desarrollo Sostenible (ODS) propuestos por la Organización de las Naciones Unidas. A continuación, se delinean los ODS más relevantes para este análisis:

- **ODS 4: Educación de calidad**. La relación entre este objetivo y el estudio realizado subraya la importancia de incorporar conocimientos financieros entre la población junto con el desarrollo de un pensamiento crítico para la toma de decisiones informadas en un panorama económico caracterizado por su volatilidad y complejidad, con el propósito de ser capaces de reconocer riesgos financieros y actuar de manera prudente en las inversiones. Aquellas personas interesadas y decididas a invertir deberían tener la oportunidad de poder llevarlo a cabo tras una educación que sea utilizada como herramienta para enfrentar y adaptarse a los desafíos financieros.
- **ODS 8: Trabajo decente y crecimiento económico**. A nivel global, la influencia de las criptomonedas y las fluctuaciones financieras asociadas a ellas en la economía pueden tener un impacto significativo en la estabilidad y crecimiento económico. Asimismo, la evolución y volatilidad de los mercados de las monedas digitales pueden afectar de manera directa a los factores resaltados en este objetivo tales como fomentar un crecimiento económico inclusivo y sostenible, empleo pleno y productivo y trabajo decente para todos.
- **ODS 12: Producción y consumo responsables**. La actividad de minería de criptoactivos, especialmente de aquellos con altos requerimientos energéticos como Bitcoin, es cuestionada respecto la sostenibilidad y el uso responsable de los recursos.
- **ODS 13: Acción por el clima**. En línea con el ODS 12, el impacto ambiental derivado de la minería de criptomonedas debido a su elevado consumo energético tiene una conexión directa con la acción climática, por lo que se deberían investigar y fomentar métodos más sostenibles dentro de dicha industria para contribuir efectivamente a la mitigación del cambio climático.
- **ODS 16: Paz, justicia e instituciones sólidas**. La estructura descentralizada y la falta de regulación inherente a las divisas digitales presentan desafíos significativos en la prevención de delitos financieros, tales como el lavado de dinero y la financiación de actividades terroristas. Por consiguiente, es imperativo el desarrollo y la implementación de un marco regulatorio adecuado para las criptomonedas, con el objetivo de promover la justicia, así como de establecer instituciones efectivas, responsables e inclusivas.
- **ODS 17: Alianzas para lograr objetivos**. Este ODS enfatiza la importancia de perseguir la cooperación internacional a través de la colaboración entre gobiernos, el sector privado y la sociedad civil, para comprender las complejidades del mercado de divisas digitales y desarrollar marcos regulatorios eficaces que promuevan una economía global más estable, segura, sostenible y equitativa.

Por ende, el estudio del trabajo realizado trasciende la esfera económica y financiera entrelazándose estrechamente con aspectos de desarrollo sostenible, equidad, sostenibilidad ambiental y gobernabilidad global.