



**UNIVERSITAS**  
*Miguel Hernández*

Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Estadística Empresarial

Trabajo de Fin de Grado Curso 2025/2026

Convocatoria Febrero

**TECNOLOGÍA BLOCKCHAIN Y CRIPTOMONEDAS: REVOLUCIÓN  
DIGITAL DEL SISTEMA FINANCIERO GLOBAL**

**Autor:** Álvaro Sarabia Belda

**Tutor:** Antonio Bolaños López

## Resumen

En los últimos años, el avance tecnológico ha transformado de forma profunda el sistema financiero mundial. Entre las innovaciones más relevantes destaca la tecnología blockchain, base de las criptomonedas y de un nuevo modelo de economía digital caracterizado por la descentralización y la transparencia.

Desde la aparición de Bitcoin en 2008, el interés por esta tecnología no ha dejado de crecer. Su objetivo inicial fue crear un sistema de pago seguro que no dependiera de bancos ni gobiernos, pero su alcance ha superado cualquier expectativa. Hoy, blockchain sustenta redes globales que permiten transferir valor, ejecutar contratos inteligentes y desarrollar aplicaciones financieras sin intermediarios.

A pesar de su potencial, las criptomonedas plantean importantes desafíos: la volatilidad de sus precios, los riesgos de seguridad y la falta de regulación en muchos países. No obstante, su expansión demuestra que estamos ante una revolución comparable a la que supuso Internet en los años noventa. Cada vez más instituciones, empresas y bancos centrales exploran su uso, impulsando incluso el desarrollo de monedas digitales oficiales (CBDC).

El objetivo de este trabajo es analizar cómo la tecnología blockchain y las criptomonedas están transformando el sistema financiero global, estudiando sus fundamentos técnicos, sus principales aplicaciones y su impacto económico, así como los retos que plantea su integración en la economía mundial.

**Palabras clave:** Blockchain, Criptomonedas, Finanzas Digitales, Descentralización, Bitcoin, DeFi, Regulación Financiera

## **Abstract**

In recent years, technological innovation has profoundly reshaped the global financial system. Among the most influential advances is blockchain technology, the foundation of cryptocurrencies and a new digital economy based on decentralization and transparency.

Since the creation of Bitcoin in 2008, interest in blockchain has grown rapidly. Originally designed as a secure, peer-to-peer payment system independent from banks or governments, it has evolved into a platform supporting global networks for value transfer, smart contracts, and decentralized finance.

Despite its potential, cryptocurrencies face challenges such as price volatility, security risks, and regulatory uncertainty. However, their expansion reveals an ongoing financial revolution that may redefine trust, value, and money itself. This paper analyzes how blockchain and cryptocurrencies are transforming the global financial system, exploring their technical foundations, economic implications, and future prospects.

**Key words:** Blockchain, Cryptocurrencies, Digital Finance, Decentralization, Bitcoin, DeFi, Financial Regulation

# ÍNDICE

<b>1. INTRODUCCIÓN</b> .....	5
1. Objeto del trabajo .....	5
2. Objetivos del Trabajo .....	5
<b>2. METODOLOGÍA UTILIZADA</b> .....	6
<b>3. EL DINERO Y SU EVOLUCIÓN</b> .....	9
3.1. Naturaleza y funciones del dinero .....	9
3.2. Etapas históricas del dinero .....	10
3.3. Tipologías actuales del dinero .....	11
<b>4. TECNOLOGÍA BLOCKCHAIN</b> .....	12
4.1. Definición y principios básicos .....	12
4.2. Tipos de Consenso y Nodos .....	13
4.3 Centralización vs Descentralización .....	15
4.4 Seguridad y criptografía .....	16
4.5 Principales desafíos y limitaciones actuales .....	18
<b>5. CRIPTOMONEDAS</b> .....	20
5.1. Origen y principios de las criptomonedas .....	20
5.2. Volatilidad y percepción del mercado .....	21
5.3. El impacto ambiental de la minería .....	23
<b>6. IMPACTO DE BLOCKCHAIN EN EL SISTEMA FINANCIERO GLOBAL</b> .....	24
6.1. Aplicaciones en pagos, inversión y finanzas descentralizadas (DeFi) .....	25
6.2. Viabilidad técnica .....	26
6.3. Viabilidad económica .....	31
6.4 Marco Legal de la UE para Blockchain y criptomonedas .....	34
<b>7. CONCLUSIÓN</b> .....	36
<b>8. BIBLIOGRAFÍA</b> .....	39

## **1. INTRODUCCIÓN**

### **1. Objeto del trabajo**

El presente trabajo tiene como objeto analizar la influencia que la tecnología blockchain y las criptomonedas ejercen sobre el sistema financiero global. La cadena de bloques, surgida con la creación del Bitcoin en 2008, representa un cambio radical en la forma de entender el dinero, la confianza y la intermediación económica. Su funcionamiento descentralizado y transparente plantea una alternativa a los modelos financieros tradicionales, dominados por bancos centrales e instituciones reguladoras.

En este sentido, el trabajo busca comprender cómo esta tecnología, originalmente pensada para las transacciones digitales entre particulares, ha evolucionado hasta convertirse en una herramienta con potencial para transformar procesos bancarios, financieros y administrativos. Además, se pretende examinar la repercusión que las criptomonedas han tenido en la economía internacional y las razones que explican su creciente adopción por parte de usuarios, empresas y gobiernos.

### **2. Objetivos del Trabajo**

El objetivo general de este estudio es identificar y evaluar los efectos de la tecnología blockchain y las criptomonedas sobre la estructura y el funcionamiento del sistema financiero mundial.

De forma más específica, los objetivos son los siguientes:

- Explicar los fundamentos técnicos de la tecnología blockchain y su relación con el origen de las criptomonedas.
- Analizar las características, ventajas y limitaciones de las principales criptomonedas del mercado actual.
- Examinar las implicaciones económicas, sociales y regulatorias que acompañan a la expansión de las criptomonedas.
- Valorar el impacto potencial de esta revolución digital en la evolución futura del dinero y de las instituciones financieras.

## 2. METODOLOGÍA UTILIZADA

El presente Trabajo de Fin de Grado se desarrolla mediante una revisión documental de carácter descriptivo–analítico, centrada en la evolución del dinero en la era digital y el impacto de la tecnología *blockchain* y los criptoactivos en el sistema financiero, incluyendo sus implicaciones económicas, operativas y regulatorias. Esta metodología permite integrar conceptos técnicos, económicos y jurídicos a partir de fuentes contrastadas, con el objetivo de construir un marco coherente que facilite la comprensión del fenómeno y sus efectos.

### 2.1. Diseño del estudio y enfoque metodológico

Se ha optado por una revisión documental debido a que el objeto de estudio — criptoactivos, *blockchain*, finanzas descentralizadas (DeFi) y el marco normativo europeo— se caracteriza por su rápida evolución y por la existencia de una amplia producción institucional, académica y divulgativa. El enfoque adoptado combina:

**Análisis conceptual**, para definir con precisión los principales conceptos (dinero, agregados monetarios, *blockchain*, tokenización, DeFi, stablecoins, CBDC).

**Análisis comparativo**, para contrastar modelos y mecanismos (por ejemplo, *Proof of Work* vs *Proof of Stake*, usos centralizados vs descentralizados, ventajas y limitaciones técnicas y económicas).

**Análisis normativo**, para describir el marco regulatorio aplicable en la Unión Europea, prestando atención a normas y organismos competentes.

La finalidad del trabajo no es la predicción de precios ni la recomendación de inversión, sino el estudio estructurado del fenómeno desde una perspectiva académica y de utilidad general.

### 2.2. Alcance, delimitación y contexto temporal

El TFG se delimita a los siguientes aspectos:

**Ámbito temático principal:** dinero digital, tecnología *blockchain*, criptoactivos (con especial atención a Bitcoin y Ethereum como referencias históricas y técnicas), DeFi, y el marco regulatorio europeo aplicado a criptoactivos.

**Ámbito geográfico:** se toma como referencia principal la Unión Europea, por su relevancia normativa (p. ej., MiCA) y por el impacto del marco regulatorio en el mercado y la protección del usuario.

Marco temporal: se consideran especialmente fuentes y documentos publicados en el periodo 2008–actualidad, al corresponder con el nacimiento de Bitcoin, la evolución de *blockchain* y el desarrollo regulatorio reciente.

### **2.3. Procedimiento de búsqueda y selección de información**

Para garantizar la trazabilidad del contenido, la información se ha recopilado a partir de un procedimiento de búsqueda y selección basado en tres bloques de fuentes, priorizando las oficiales y académicas para definiciones, datos y regulación:

#### **Fuentes oficiales e institucionales (prioritarias)**

Se emplean para: definiciones económicas (dinero, agregados), documentos sobre estabilidad financiera, criptografía/finanzas digitales, y especialmente normativa y supervisión.

Ejemplos de este bloque incluyen: organismos de la UE y repositorios legales, bancos centrales, organismos supervisores y documentos institucionales.

#### **Fuentes académicas y técnicas (complementarias)**

Se utilizan para: fundamentos de *blockchain*, explicación de mecanismos de consenso, *smart contracts*, escalabilidad, y evolución tecnológica. Se incluyen *papers*, documentos técnicos y literatura especializada que permitan sustentar el marco conceptual con rigor.

#### **Fuentes generales y divulgativas (de apoyo)**

Se emplean únicamente para: contextualizar conceptos de forma accesible, ilustrar ejemplos y ayudar a presentar ideas complejas de forma clara. Estas fuentes no se utilizan como base principal para afirmaciones regulatorias o conclusiones críticas sin contraste con fuentes oficiales o académicas.

## **2.4. Criterios de inclusión y exclusión de fuentes**

Para asegurar la calidad de la revisión, se aplicaron los siguientes criterios:

### **Criterios de inclusión**

Documentos de organismos oficiales (UE, bancos centrales, autoridades supervisoras) para regulación, definiciones y directrices.

Literatura académica y técnica relevante para los aspectos tecnológicos y económicos del objeto de estudio.

Fuentes generales con autoría clara y contenido estable, utilizadas de manera complementaria para mejorar la claridad expositiva.

Fuentes actualizadas o de referencia histórica cuando sean esenciales (p. ej., documentos fundacionales como el *whitepaper* de Bitcoin).

### **Criterios de exclusión**

Contenidos sin autor o sin fecha identificable cuando impidan evaluar su fiabilidad.

Entradas puramente promocionales o de carácter comercial sin respaldo documental.

Opiniones no contrastadas que no permitan extraer definiciones o información verificable.

Fuentes redundantes cuando existen documentos más completos u oficiales.

## **2.5. Organización y tratamiento de la información**

La información seleccionada se organizó por bloques temáticos, siguiendo la estructura del trabajo.

Se realizó una lectura crítica de cada fuente, extrayendo definiciones, ideas clave y evidencias relevantes, y contrastando afirmaciones especialmente sensibles (por ejemplo, aspectos regulatorios, impactos sistémicos o riesgos) con documentación oficial siempre que fue posible. Finalmente, todas las fuentes empleadas se referencian en el apartado de Bibliografía siguiendo el formato APA, con el objetivo de garantizar transparencia y trazabilidad.

### 3. EL DINERO Y SU EVOLUCIÓN

#### 3.1. Naturaleza y funciones del dinero

El dinero puede entenderse como un mecanismo social de coordinación que reduce los costes de intercambio y permite la especialización. Cumple cuatro funciones clásicas: medio de intercambio (evita la doble coincidencia del trueque), unidad de cuenta (estandariza valores), depósito de valor (traslada poder adquisitivo en el tiempo) y estándar de pagos diferidos (facilita contratos Inter temporales). Para funcionar bien necesita aceptación generalizada, escasez creíble, divisibilidad, durabilidad, portabilidad, uniformidad y verificabilidad.

En la práctica opera una jerarquía monetaria: en la cúspide, el dinero del banco central (billetes/monedas y reservas); por debajo, el dinero bancario (depósitos a la vista) convertible a la par; y, en niveles inferiores, instrumentos de cuasi-dinero privados. Los bancos centrales miden la oferta monetaria mediante agregados: M1 (efectivo + depósitos a la vista), M2 (M1 + depósitos a plazo/cuentas con preaviso), etc. (*Banco central Europeo, n.d.*)

*Figura 1: Imagen moneda antigua*



*Fuente: noticiastrabajo*

### 3.2. Etapas históricas del dinero

a) Trueque y dinero mercancía. Antes del dinero, el intercambio exigía coincidencia de necesidades. Para reducir fricciones se usaron bienes de amplia aceptación (sal, metales, conchas, granos), que actuaron como dinero mercancía gracias a su valor y propiedades físicas.

b) Monetización metálica y acuñación (s. VII a. C. – Edad Moderna). La acuñación de monedas metálicas (electro, oro, plata, cobre) estandarizó pesos y calidades, bajando costes de verificación. La autoridad emisora obtenía señoreaje y, en crisis, recurría al debilitamiento (menor fino), con efectos en precios y confianza.

c) Dinero representativo y billetes convertibles. Los recibos de depositarios y bancos sobre metales evolucionaron a billetes convertibles a demanda. La banca a reservas fraccionarias expandió el crédito, impulsando actividad, pero también episodios de pánicos y corridas.

d) Patrón oro y colapso (finales s. XIX – 1931). La fijación de paridades al oro estabilizó precios y facilitó comercio, pero mostró rigideces ante choques y guerras. Tras suspensiones y ajustes, el sistema se desarticuló entre guerras.

e) Bretton Woods y transición al dinero fiduciario (1944–1971). Tras la II Guerra Mundial se fijaron tipos de cambio anclados al dólar, convertible en oro sólo para bancos centrales. En agosto de 1971, la suspensión de la convertibilidad (conocida como Nixon shock) precipitó el fin del régimen y la generalización del dinero fiduciario.

f) Digitalización de pagos (1980–2010). Tarjetas, cajeros y banca en línea consolidaron que el dinero usado por hogares y empresas existe sobre todo como apuntes contables en sistemas bancarios.

g) Nuevas formas digitales (2010–presente). Con Bitcoin (2008–09) surgen criptoactivos sin emisor central; proliferan pagos móviles y stablecoins privadas; bancos centrales exploran CBDC (monedas digitales de banco central) con distintos diseños.

### **3.3. Tipologías actuales del dinero**

El dinero actual puede verse desde tres ángulos que se solapan: quién lo emite, qué lo respalda y cómo se registra. Esta mirada ayuda a comparar formas tradicionales y digitales, entendiendo sus ventajas, límites e impacto financiero.

#### **3.3.1. Según el emisor**

**Dinero público:** Incluye el efectivo y las reservas en el banco central. Sirve de referencia última de valor y es el activo más seguro del sistema. En varios países se estudia una versión digital accesible al público para combinar la solidez estatal con funcionalidades electrónicas.

**Dinero privado:** Abarca los depósitos bancarios usados a diario (transferencias, tarjetas), convertibles a la par en dinero del banco central. Se suman saldos electrónicos de entidades de pago (billeteras, prepago) y criptoactivos emitidos por agentes no soberanos, entre ellos stablecoins orientadas a mantener paridad con una moneda o activo.

#### **3.3.2. Según el respaldo o forma de valor**

**Fiduciario (fiat):** Monedas oficiales cuyo valor descansa en su aceptación legal y en la credibilidad del emisor público.

**Representativo:** Instrumentos con convertibilidad explícita a un activo (reservas seguras, mercancías); su solidez depende del respaldo y del canje.

**Criptoactivos sin paridad:** Unidades de redes descentralizadas regidas por protocolo, sin promesa de conversión a fiat; su precio lo marca el mercado.

#### **3.3.3. Según el soporte y la tecnología de registro**

**Físico:** Monedas y billetes, sencillos, sin intermediarios y resilientes ante fallos electrónicos.

**Contable-electrónico:** Dinero como apuntes en cuenta liquidado en infraestructuras centralizadas (RTGS, redes de tarjetas, transferencias inmediatas).

Token digital: Propiedad verificada criptográficamente en DLT o plataformas cerradas: incluye criptoactivos nativos, tokenización de depósitos/activos y posibles diseños de dinero público digital (por token o por cuenta).

## **4. TECNOLOGÍA BLOCKCHAIN**

### **4.1. Definición y principios básicos**

La tecnología blockchain (*Binance academy, n.d.*), es en esencia, un libro de contabilidad digital que registra de manera segura y transparente una serie de transacciones en bloques enlazados de forma cronológica y encriptada. Cada bloque contiene datos de transacciones, un sello de tiempo y una referencia al bloque anterior, lo que asegura la integridad y la inmutabilidad de la información almacenada en la red.

La descentralización es uno de los principios fundamentales de la tecnología blockchain, puesto que, a diferencia de los sistemas tradicionales de bases de datos centralizadas, donde una autoridad central ejerce control sobre la información, la blockchain opera como una red descentralizada de nodos interconectados. Este tipo de estructura elimina la necesidad de un intermediario confiable y brinda mayor seguridad y resistencia a la manipulación o corrupción de los datos, ya que cualquier cambio en la cadena requiere el consenso de la mayoría de los nodos de la red.

La historia de las criptomonedas y la tecnología blockchain se remonta a la creación de Bitcoin por un individuo o grupo conocido como Satoshi Nakamoto en 2008. Bitcoin, la primera criptomoneda descentralizada, introdujo la blockchain como un sistema de registro distribuido para transacciones de valor, sentando las bases para el desarrollo de nuevas criptomonedas y aplicaciones blockchain en los años siguientes. Desde entonces, la tecnología blockchain ha evolucionado significativamente, con Ethereum y otras plataformas líderes ampliando el alcance y la funcionalidad de la blockchain más allá de las transacciones financieras, abriendo nuevas posibilidades en áreas como la gestión de identidad, la trazabilidad de productos, la gobernanza descentralizada y más

Ethereum, una de las plataformas de blockchain más influyentes y ampliamente utilizadas, ha desempeñado un papel crucial en la evolución y la expansión de la tecnología blockchain. Lanzado en 2015 por el programador Vitalik Buterin y respaldado por la Fundación Ethereum, introdujo una nueva dimensión a la blockchain al permitir la ejecución de contratos inteligentes, así como el desarrollo de aplicaciones descentralizadas sobre su infraestructura. Los contratos inteligentes son programas informáticos autónomos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas, lo que permite la automatización de procesos y la creación de servicios descentralizados.

#### **4.2. Tipos de Consenso y Nodos**

Dentro de la arquitectura blockchain, los algoritmos de consenso son el corazón que impulsa la fiabilidad y la eficiencia de las transacciones y del mantenimiento de registros dentro de la red descentralizada. Estos algoritmos no solo validan las transacciones y mantienen la coherencia de la cadena, sino que también aseguran que todas las copias de la blockchain sean consistentes.

El Proof of Work (PoW) (*Binance academy, n.d.*) es uno de los algoritmos más antiguos y conocidos, utilizado por Bitcoin y muchas otras criptomonedas. Implica que los nodos llamados “mineros” compitan entre sí para resolver un “problema criptográfico” complejo que requiere un considerable poder computacional al que se le destinan amplios recursos. El primer minero que resuelve este problema obtiene el derecho de añadir un nuevo bloque a la cadena y, como recompensa, recibe una cantidad específica de la criptomoneda. Aunque este método ha demostrado ser efectivo en mantener la red segura y descentralizada, también ha sido objeto de críticas por el amplio gasto energético que implica y por fomentar una centralización no deseada, ya que los mineros con mayor capacidad de cómputo tienen más probabilidades de resolver el problema primero.

Como contrapartida al Pow, se encuentra el el Proof of Stake (PoS) (*Binance academy, n.d.*), que ofrece una alternativa más eficiente. Aquí la probabilidad de validar un bloque

y recibir la recompensa no depende de la capacidad de nuestro sistema, sino de la cantidad de monedas que el validador posee y está dispuesto a "poner en juego" más conocido como "stakear" o dejar bloqueados sus activos, reduce además la posibilidad de ataques de malos actores en la red, ya que necesitarían contar una gran cantidad de activos para tener una oportunidad significativa de influir en el consenso global, lo que supondría un gran riesgo financiero para el atacante, casi inviable como se ha comprobado en diversas ocasiones a lo largo de los años (*BeInCrypto, n.d.*).

El Proof of Authority (PoA) es otro tipo de algoritmo que está ganando popularidad, especialmente en aplicaciones empresariales. En PoA, las transacciones y la creación de nuevos bloques están controladas por nodos validadores "pre-aprobados", conocidos como autoridades. Estos nodos son seleccionados según su reputación y fiabilidad que poseen, este modelo ha sido objeto de críticas pues puede parecer que reintroduce un cierto grado de centralización, pero es muy efectivo para situaciones donde la privacidad y la eficiencia de la transacción son críticas.

En el gráfico se comparan los diferentes tipos de consenso que hemos hablado:

**Proof of Work (PoW):** Alta seguridad, pero con un alto consumo energético, ejemplificado por Bitcoin.

**Proof of Stake (PoS):** Eficiente en términos energéticos, aunque presenta riesgos de concentración de poder. Ethereum 2.0 es un caso típico de uso.

**Proof of Authority (PoA):** Rápido y escalable, pero con menor descentralización, comúnmente utilizado en redes corporativas.

Figura 2: Imagen diferencias de los tipos de consenso

Tipo de Consenso	Ventajas	Desventajas	Casos de Uso Típicos
<b>Proof of Work</b>	Alta Seguridad	Alto consumo energético	Bitcoin
<b>Proof of Stake</b>	Eficiencia Energética	Riesgo de concentración de poder	Ethereum 2.0
<b>Proof of Authority</b>	Rápido y escalable	Menor descentralización	Redes corporativas

Fuente: Elaboración propia

### 4.3 Centralización vs Descentralización

El debate entre centralización y descentralización es clave para entender por qué las criptomonedas aportan ciertos beneficios. En esta sección contrastamos las ventajas de los modelos descentralizados con los retos propios de los sistemas centralizados.

La centralización implica que una autoridad única supervisa y controla las operaciones de los usuarios. Durante mucho tiempo, por ejemplo, dependíamos de Correos para enviar cartas y de los bancos para mover dinero; esa intermediación nos hacía estar sujetos a sus condiciones, horarios y comisiones, generando una evidente dependencia. Estos arreglos institucionales respondieron a una necesidad básica: contar con seguridad y confianza en las transacciones de bienes y servicios.

En general, las personas buscamos mecanismos fiables para operar, y las entidades centralizadas surgieron precisamente para proporcionar ese amparo y certidumbre.

Si bien las nuevas tecnologías e Internet han revolucionado muchos aspectos de nuestra vida, aún podemos observar ciertos grados de centralización dentro de él. Por ejemplo, en el e-commerce, es común recurrir a plataformas prestigiosas como Amazon en lugar de otras tantas opciones existentes. Esto es debido a la sensación de seguridad que ofrecen las grandes empresas. Esta tendencia muestra cómo la centralización sigue siendo un

aspecto muy interiorizado en la psicología humana, y que nos hace siempre buscar la seguridad en las transacciones que realizamos.

No obstante, también se ha allanado el camino para la descentralización gradual de numerosos aspectos, estamos avanzando hacia un futuro donde no necesitaremos intermediarios para la mayoría de nuestras transacciones y las criptomonedas son un ejemplo destacado de este movimiento hacia la descentralización. Podemos realizar transacciones de igual a igual (P2P) o B2B, de manera segura y eficiente, sin depender de intermediarios como bancos o instituciones financieras.

Gran parte de esta ayuda provendrá de los contratos inteligentes, pues si compramos un producto y no lo recibimos, el contrato no verificará la transacción y el vendedor no podrá recibir el pago de forma automática, proporcionando así una capa adicional de seguridad y protección para los usuarios.

#### **4.4 Seguridad y criptografía**

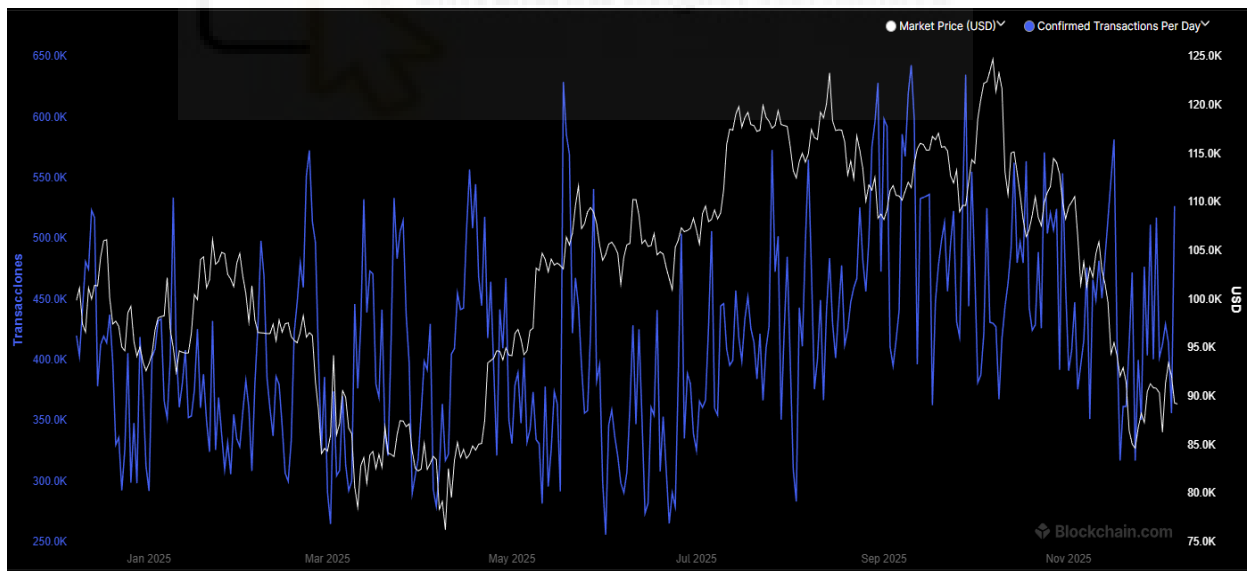
La criptografía es esencial para la funcionalidad y seguridad de la blockchain. Actúa como la primera línea de defensa contra los intentos de fraude y asegura que todas las transacciones sean autorizadas y permanentes una vez confirmadas. La criptografía se utiliza de varias maneras dentro de la blockchain, incluyendo la creación de hashes, la firma digital de transacciones, y la verificación de la integridad y autenticidad de la información.

Cada transacción es firmada digitalmente por el remitente utilizando su clave privada. Esta firma es esencialmente un mecanismo que se asegura de que la transacción no pueda ser alterada una vez emitida, cada cambio invalidaría la firma por completo. Cuando los nodos reciben una transacción, utilizan la clave pública del remitente para verificar la firma; si la verificación es correcta, la transacción es considerada auténtica y puede ser procesada.

Además de las firmas digitales, la integridad de los bloques en la cadena se mantiene a través del uso de funciones de hash criptográfico. Cada bloque contiene su propio hash y el hash del bloque anterior, lo cual crea una cadena dependiente donde cada bloque nuevo refuerza la seguridad de los bloques anteriores. Modificar cualquier información en un bloque anterior requeriría recalcular no solo su hash sino también el de todos los bloques, algo computacionalmente imposible a día de hoy, lo que asegura la inmutabilidad de la red.

Las criptomonedas, usan la criptografía no solo para asegurar las transacciones sino también para generar y verificar la identidad digital de los usuarios a través de sus carteras digitales o 'wallets' (Binance Academy, n. d.). Estas wallets generan y almacenan las claves privadas de los usuarios de manera segura, permitiéndoles realizar transacciones en la red sin revelar su identidad lo cual es una característica clave que proporciona privacidad y seguridad a los usuarios.

Figura 3: Número de transacciones confirmadas por día durante el 2025



Fuente: Blockchain.com

## 4.5 Principales desafíos y limitaciones actuales

Pese a sus numerosos beneficios, son varios los desafíos significativos que pueden obstaculizar la eficiencia y efectividad, principalmente nos enfrentamos a los siguientes: la complejidad logística, las diversas regulaciones y normativas de cada país, y los peligrosos fraudes y dificultades en la seguridad. Vamos a analizarlos uno a uno comprendiendo lo beneficioso que podría ser el uso de la blockchain en cada caso:

### Complejidad Logística

La complejidad logística es una de las principales barreras en la actualidad. Esta complejidad abarca una amplia gama de desafíos relacionados con la gestión, coordinación y ejecución de actividades logísticas a lo largo de toda la cadena de suministro global. Desde la planificación y adquisición de materias primas hasta la entrega final de productos al consumidor, cada etapa del proceso logístico puede verse afectada por diversos factores.

Una de las principales fuentes de complejidad es la diversidad de partes involucradas. Las empresas globales deben coordinar sus actividades con proveedores, fabricantes, distribuidores y transportistas en diferentes países y regiones. Esto crea complicaciones como la coordinación de horarios, la comunicación efectiva y la correcta gestión de responsabilidades.

Además, el cruce de fronteras internacionales introduce complicaciones adicionales como el cumplimiento de normativas aduaneras y la gestión de documentos de exportación e importación. Las empresas deben lidiar con una gran cantidad de documentación y regulaciones que varían de un país a otro, lo que puede retrasar los envíos y aumentar los costes. Es pues, que se requiere una respuesta a la altura de una tecnología nueva e innovadora como es la Blockchain.

## **Regulaciones y Normativas**

Las leyes y requisitos de cada país constituyen otro elemento fundamental, ya que abarcan un amplio rango de ámbitos como el comercio de bienes y servicios, la gestión aduanera...

Los empresarios deben estar constantemente informados sobre este entramado de reglas que regulan el intercambio internacional, especialmente cuando se trata de operaciones con países fuera de la Unión Europea.

Este conjunto de exigencias legales puede resultar costoso y complejo para las compañías, sobre todo para las que se inician en el comercio exterior y/o operan con múltiples países. Además, las regulaciones pueden emplearse como instrumentos políticos y económicos para defender los intereses nacionales y reforzar la competitividad de las empresas locales.

Por ejemplo, los aranceles y las cuotas de importación pueden servir para restringir la entrada de productos extranjeros en el mercado interno y ofrecer protección a los productores nacionales frente a la competencia exterior. De igual forma, las barreras técnicas al comercio, como las condiciones de etiquetado o de certificación, pueden utilizarse para poner obstáculos adicionales al acceso de mercancías foráneas al mercado nacional.

## **Fraude y Seguridad**

Como última preocupación dentro de esta sección tenemos el fraude y la seguridad, peligros en gran parte digitales con la falsificación de documentos, robo de identidad, manipulación de las transferencias bancarias, etc. Esto puede desencadenar pérdidas grandes de mercancía, tiempo y dinero en trámites legales internacionales para ganar una disputa.

El fraude es una práctica desgraciadamente bastante común y es uno de los puntos flojos de la blockchain. Y ya no por falta de seguridad en su funcionamiento, sino en las estafas y fraudes en los que un usuario inexperto puede caer, son decenas las que se cometen a diario en el entorno de criptomonedas, y pese a no deber tener ningún problema, ya que

en este ámbito de transacciones internacionales únicamente trabajaríamos con smart contracts verificados y destinados específicamente a dicho uso, la gestión de los fondos puede ser un problema por resolver.

No obstante, una correcta gestión de nuestra seguridad digital y la manera en la que se gestionan los fondos debería ser más que suficiente para no caer en este tipo de estafas.

## **5. CRIPTOMONEDAS**

### **5.1. Origen y principios de las criptomonedas**

El origen de las criptomonedas no se limita a la aparición de Bitcoin en 2008, sino que hunde sus raíces en varios intentos previos de crear dinero electrónico seguro. En la década de 1980, el criptógrafo David Chaum desarrolló eCash, un sistema de dinero digital anónimo basado en técnicas criptográficas, considerado uno de los primeros precedentes del dinero electrónico moderno. Más tarde, en los años noventa, surgieron proyectos como Hashcash, de Adam Back, un mecanismo de proof-of-work pensado para combatir el spam y los ataques de denegación de servicio, que después inspiraría el sistema de minería de Bitcoin.

El punto de inflexión llega en 2008, cuando una persona o grupo bajo el seudónimo de Satoshi Nakamoto publica el whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System”, (*Investopedia, n.d.*) en el que se propone un sistema de efectivo electrónico que permite enviar pagos directamente entre usuarios sin pasar por una entidad financiera, resolviendo el problema del doble gasto mediante una red P2P y un registro distribuido de transacciones. Según recoge el INCIBE (*INCIBE, n.d.*), el 31 de octubre de 2008 se presenta formalmente la propuesta y el 3 de enero de 2009 se mina el bloque génesis, con el que comienza a funcionar la red de Bitcoin y, seguidamente, la primera criptomoneda descentralizada.

A partir de ese momento se consolidan los principios fundamentales que caracterizan a las criptomonedas: la descentralización (la ausencia de una autoridad emisora única, sustituyéndola por una red de nodos que siguen un protocolo de consenso), el uso intensivo de la criptografía de clave pública y privada para garantizar la propiedad y la autenticidad de las transacciones, el mantenimiento de un registro distribuido o blockchain que aporta transparencia y dificulta la manipulación de datos, y la existencia de una emisión programada y limitada (como el máximo de 21 millones de bitcoins) que introduce la idea de “escasez digital”. En conjunto, estos elementos explican por qué las criptomonedas se presentan como una alternativa al dinero fiduciario tradicional y se consideran una posible revolución en la forma de entender el dinero y el sistema financiero global (INCIBE, n.d.).

## **5.2. Volatilidad y percepción del mercado**

La volatilidad es (*Coinbase, n.d.*) una medida de cuánto ha subido o bajado el precio de un activo en particular con el tiempo. Por lo general, cuanto más volátil es un activo, más arriesgado se considera como inversión y más potencial tiene para ofrecer mayores rendimientos o mayores pérdidas en períodos de tiempo más cortos que los activos comparativamente menos volátiles.

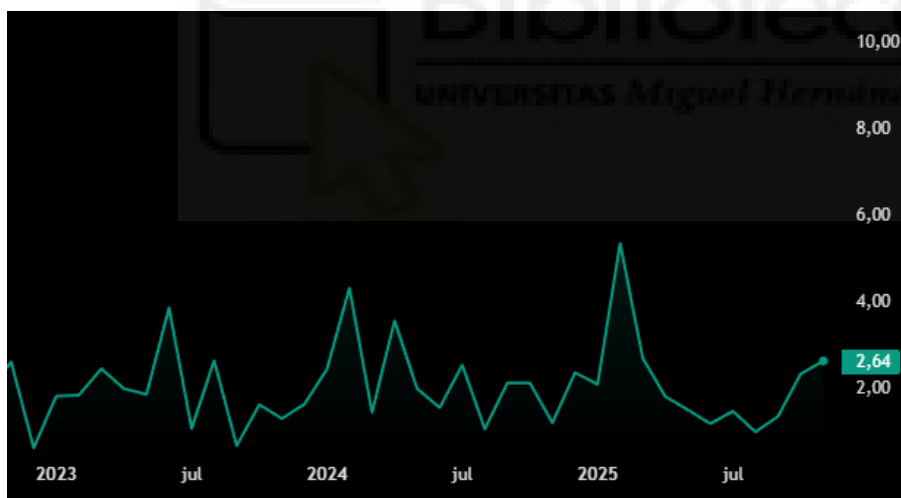
Como tipo de activo más reciente, se considera que las criptomonedas son volátiles, con un potencial de movimientos significativos al alza y a la baja en periodos de tiempo cortos. Se considera que las acciones tienen una amplia gama de volatilidad, desde la relativa estabilidad de las acciones de gran capitalización (como Apple o Berkshire Hathaway) hasta las a menudo erráticas acciones de centavo. Los bonos, por el contrario, se consideran un activo de menor volatilidad, y normalmente experimentan oscilaciones al alza y a la baja menos drásticas que tienen lugar en plazos más largos.

Un factor determinante (*BBVA, n.d.*) en la fluctuación del precio de las criptomonedas es su baja adopción. Una adopción masiva ayudaría a regularlo, pero, por un lado, su equiparación a las monedas fiduciarias no es total, ya que aún no tienen su facilidad para ser intercambiadas por productos y servicios ni la capacidad de constituir una reserva de valor estable, es decir, no garantizan que puedan mantener su poder adquisitivo en el largo plazo. Por otro lado, el aumento progresivo de la regulación, como por ejemplo MiCA

(Boletín Oficial del Estado, 2023) en la Unión Europea, podría sentar las bases para una mayor adopción; aunque, si la regulación es demasiado estricta, podría tener el efecto contrario.

Otro factor importante es la confianza. Las criptomonedas surgieron con el objetivo de descentralizar la gestión de los fondos de los particulares, por lo que caen fuera del control de las instituciones financieras. Esta independencia implica que su valor no está respaldado por los gobiernos centrales. Por lo tanto, los mercados no confían tanto en las criptomonedas como en las monedas fiduciarias, cuya oferta e inflación están controladas por los bancos centrales. Las ‘stablecoins’ quieren ganar parte de esta confianza controlando su fluctuación mediante algoritmos o bien vinculándola a la de una moneda fiduciaria, activos materiales (oro, inmuebles) u otra criptomoneda, lo cual las hace menos volátiles. Un ejemplo de ello es USD Coin, ligada al dólar estadounidense, que está sujeta a auditorías y regulada por la Red de Control de Delitos Financieros del Gobierno de Estados Unidos.

Figura 4: Imagen volatilidad bitcoin desde el 2023



Fuente: [tradingview.com](https://tradingview.com)

### **5.3. El impacto ambiental de la minería**

El minado de criptomonedas es el proceso fundamental que sostiene el funcionamiento de las redes descentralizadas basadas en blockchain, como Bitcoin y Ethereum. En esencia, el minado implica la validación y registro de transacciones en bloques de datos, asegurando la integridad y seguridad de la red. Los mineros utilizan potentes equipos informáticos para resolver complejos problemas matemáticos, que verifican las transacciones y añaden nuevos bloques a la cadena de bloques.

A cambio de su trabajo, los mineros son recompensados con nuevas unidades de la criptomoneda en cuestión, así como con tarifas de transacción. Este proceso es esencial para garantizar la transparencia y la confianza en las transacciones, ya que elimina la necesidad de un intermediario centralizado.

El proceso intensivo de cálculo requerido para el minado de criptomonedas demanda una cantidad exorbitante de energía eléctrica. Los mineros utilizan potentes equipos informáticos que operan las 24 horas del día, los 7 días de la semana, consumiendo una cantidad significativa de electricidad. Este consumo energético a menudo se compara con el de países enteros o industrias importantes, lo que plantea preocupaciones sobre la sostenibilidad a largo plazo y el acceso equitativo a los recursos energéticos.

El uso extensivo de energía eléctrica en el minado de criptomonedas conlleva emisiones significativas de carbono, contribuyendo al calentamiento global y al cambio climático. Además, la generación de energía eléctrica suele implicar la quema de combustibles fósiles, por lo que se liberan contaminantes atmosféricos y otros gases invernadero que tienen impactos adversos en la calidad del aire y la salud humana.

El minado de criptomonedas también puede dar lugar al agotamiento de recursos naturales, como el agua y los metales preciosos utilizados en la fabricación de equipos informáticos. La extracción de estos recursos puede tener consecuencias ambientales devastadoras, incluida la degradación del hábitat, la contaminación del agua y la pérdida de biodiversidad.

*Figura 5: Imagen granja de minería*



*Fuente: elDiario.es*

## **6. IMPACTO DE BLOCKCHAIN EN EL SISTEMA FINANCIERO GLOBAL**

La tecnología blockchain ha generado uno de los cambios más significativos en la estructura financiera contemporánea desde la creación de internet. Su capacidad para eliminar intermediarios, aumentar la transparencia, mejorar la seguridad y reducir los costes operativos está impulsando una transformación profunda en la forma en que se gestionan los pagos, los activos y los servicios financieros. Tanto el sector privado como gobiernos e instituciones internacionales reconocen su potencial para redefinir la infraestructura financiera global, promoviendo nuevos modelos de negocio y ampliando el acceso a servicios financieros a regiones tradicionalmente excluidas. Al mismo tiempo, la aparición de las finanzas descentralizadas (DeFi) y los activos digitales está cuestionando el rol tradicional de bancos, aseguradoras y mercados de capitales.

## 6.1. Aplicaciones en pagos, inversión y finanzas descentralizadas (DeFi)

### Pagos y remesas internacionales

Blockchain permite realizar transacciones rápidas, seguras y con costes significativamente inferiores a los métodos tradicionales.

Ventajas clave:

- Eliminación de intermediarios como bancos corresponsales.
- Reducción del tiempo de liquidación de días a minutos.
- Costes de transacción más bajos, especialmente relevante en remesas globales. Empresas como Ripple, Circle (USDC) o redes como Lightning Network en Bitcoin han demostrado su eficacia en este ámbito.

### Tokenización de activos

La tokenización consiste en convertir activos reales (inmuebles, acciones, materias primas...) en tokens digitales que pueden negociarse fácilmente en una blockchain.

Impactos:

- Aumento de liquidez en mercados tradicionalmente ilíquidos.
- Acceso fraccionado a inversiones, democratizando la participación.
- Mayor eficiencia en la emisión, custodia y transferencia de activos.

### Finanzas Descentralizadas (DeFi)

Las DeFi representan una nueva arquitectura financiera basada en smart contracts, principalmente en redes como Ethereum. Servicios más relevantes:

- Préstamos descentralizados (Aave, Compound).
- Intercambios de criptomonedas sin intermediarios (Uniswap, Curve).
- Stablecoins algorítmicas o respaldadas por activos.
- Derivados, seguros descentralizados y gestión automatizada de carteras (Yearn Finance, Synthetix).

Impacto en el sistema financiero:

- Democratización del acceso al crédito y la inversión.
- Eficiencia operativa y reducción de costes.
- Eliminación de intermediarios bancarios tradicionales.

- Mayor inclusión financiera en regiones sin banca convencional.

Sin embargo, la falta de regulación clara y la naturaleza experimental del ecosistema también generan riesgos significativos (que se tratan en el punto 6.2).

### **Pagos con monedas digitales de bancos centrales (CBDC)**

Numerosos países (UE, China, EEUU, Brasil, etc.) estudian o prueban versiones digitales de sus monedas oficiales basadas en tecnologías inspiradas en blockchain. Las CBDC podrían:

- Mejorar la eficiencia de pagos minoristas y mayoristas.
- Proporcionar dinero programable con usos específicos.
- Facilitar políticas monetarias más precisas.

## **6.2. Viabilidad técnica**

Desde una perspectiva técnica, pueden identificarse diversas limitaciones a la hora de aplicar la tecnología blockchain. El fraude y los problemas de seguridad constituyen retos habituales en el ámbito de las transacciones y operaciones comerciales a escala global. Prácticas como la usurpación de identidad o la falsificación de documentos de pago y autorizaciones son frecuentes, y aunque la blockchain ofrece mecanismos de verificación que permiten mitigar muchos de estos riesgos, no los elimina por completo.

Por ejemplo, la manipulación de documentos o la falsificación de comprobantes se vería dificultada gracias a la validación criptográfica inherente a la cadena de bloques, mientras que los pagos podrían asegurarse mediante smart contracts que retengan los fondos hasta que se cumplan las condiciones previamente acordadas. Sin embargo, aplicar la blockchain de manera generalizada no es tan sencillo como podría parecer a primera vista. Existen varios motivos que complican su implantación de forma unilateral y total.

En primer lugar, está el factor de la seguridad. Aunque la blockchain ha demostrado ser una tecnología robusta y fiable para la transmisión descentralizada de información y valor, el desafío no reside en su funcionamiento interno, sino en las amenazas externas. La gran cantidad de estafas que se producen diariamente en el entorno digital constituye

un riesgo considerable, especialmente para usuarios sin experiencia. Estos pueden ser víctimas de engaños que les lleven a perder sus fondos sin posibilidad de recuperación, dada la ausencia de intermediarios o mecanismos tradicionales de protección y garantía.

Todos conocemos ese tipo de mensajes que llegan directamente a nuestro teléfono móvil (*The Objective, 2024*), en los que organizaciones criminales intentan ganarse nuestra confianza para obtener acceso a datos bancarios mediante técnicas de suplantación de identidad. Las personas que operan con criptomonedas, así como los aficionados que siguen las novedades del sector a través de plataformas como YouTube o Twitter, deben extremar aún más la precaución. Si ya son habituales los intentos de estafa a través de mensajería tradicional, el número de engaños relacionados con criptomonedas (*CoinSpeaker, n.d.*), en los que se emplean todo tipo de suplantaciones, es todavía mayor.

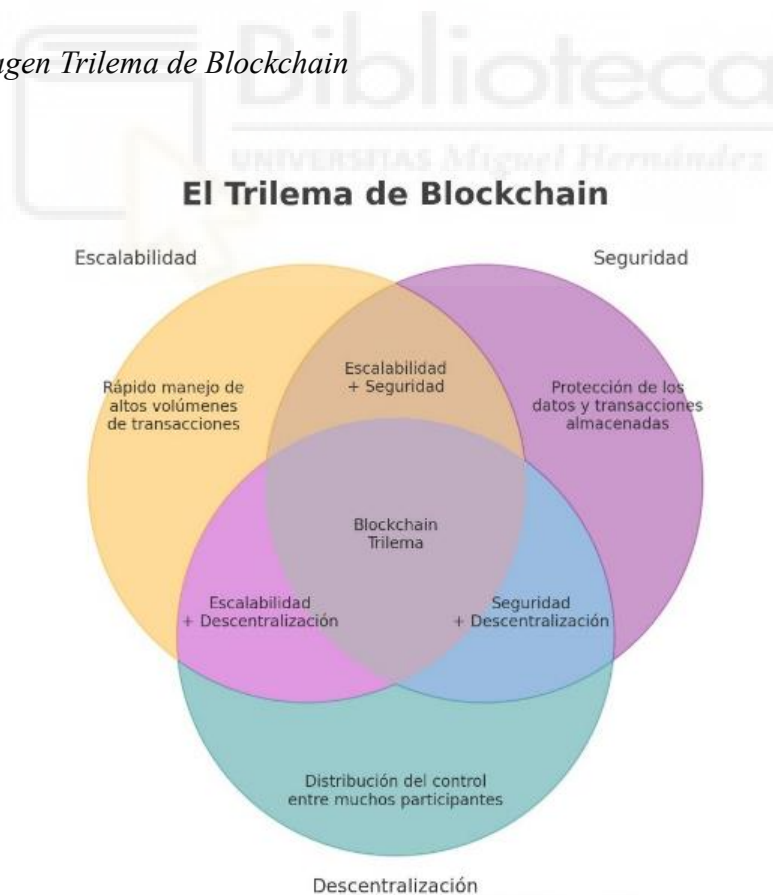
Por este motivo, es necesario tener en cuenta esta desventaja a la hora de valorar la implantación de la tecnología blockchain, aunque no se trate de un fallo propio de la tecnología. La gestión inadecuada y la falta de medidas de seguridad en la administración de fondos digitales pueden convertirse en un problema significativo para empresarios que operen en un ecosistema aún en desarrollo, donde las posibilidades de recuperar los activos perdidos son muy limitadas y, en la mayoría de los casos, prácticamente inexistentes.

Las plataformas de blockchain más conocidas, como Bitcoin o Ethereum, presentan limitaciones en cuanto al número de transacciones que pueden procesar por segundo. Esta restricción supone un obstáculo relevante en contextos de comercio internacional, donde el volumen operativo es considerablemente elevado. No obstante, han surgido diversas innovaciones que buscan aliviar estos problemas de escalabilidad, como las soluciones de segunda capa, que permiten ejecutar transacciones fuera de la cadena principal (off-chain) antes de registrarlas definitivamente en la blockchain, o el empleo de cadenas paralelas capaces de distribuir la carga de trabajo.

Más allá de los desafíos asociados a la gestión de la seguridad por parte del usuario, resulta esencial abordar las limitaciones intrínsecas de la propia tecnología blockchain. Este debate lleva años presente y no surge únicamente al plantear casos de uso como el actual, en el que tratamos de adaptar la cadena de bloques a las necesidades específicas del sistema financiero global.

El debate al que nos referimos es el denominado “trilema” (*Binance Academy, n.d.*), un concepto que ganó popularidad hace algunos años gracias a Vitalik Buterin, cofundador de la blockchain Ethereum. Según su planteamiento, resulta extremadamente complejo, si no imposible, que una blockchain pueda optimizar al mismo tiempo tres características esenciales: la descentralización, la seguridad y la escalabilidad. A continuación, analizaremos cómo se relacionan estos tres elementos entre sí tomando como referencia un esquema explicativo:

Figura 6: Imagen Trilema de Blockchain



Fuente: Elaboración propia

- **Escalabilidad (círculo naranja):** Hace referencia a la capacidad de una blockchain para manejar un alto volumen de transacciones por segundo sin comprometer su rendimiento. En el ámbito del comercio internacional, para que esta tecnología pudiera utilizarse en aplicaciones con un gran número de solicitudes (como ocurre en los sistemas de pago globales) sería imprescindible procesar transacciones de forma rápida y eficiente.
- **Seguridad (círculo morado):** Se trata de la capacidad de la red para protegerse frente a ataques y garantizar la integridad de la información. Esto incluye la prevención de fraudes, la resistencia frente a intentos de hackeo y la garantía de que las transacciones, una vez validadas, no pueden ser modificadas o alteradas.
- **Descentralización (círculo verde):** Consiste en distribuir el control de la red entre múltiples participantes, evitando que una única entidad pueda influir o dominar el sistema. La descentralización incrementa la resistencia a la censura y elimina intermediarios, lo que refuerza la confianza al repartir el poder de decisión entre todos los nodos de la red.

En las intersecciones se muestran los compromisos entre las distintas características:

- Escalabilidad + Seguridad
- Escalabilidad + Descentralización
- Seguridad + Descentralización

### **Más Escalabilidad, Menos Seguridad**

Para incrementar la escalabilidad y gestionar un volumen elevado de transacciones, suele ser necesario simplificar los mecanismos de consenso. Esto permite procesar las operaciones con mayor rapidez, pero a cambio puede afectar a la seguridad, ya que se reduce el número de verificaciones y validaciones que cada transacción debe superar. Esta disminución en los controles abre la puerta a que posibles atacantes identifiquen y exploten vulnerabilidades dentro de la red.

### **Más Descentralización, Menos Escalabilidad**

Incrementar la descentralización implica que un mayor número de participantes intervenga en la verificación de las transacciones. Este enfoque resulta beneficioso para la red, pues distribuye el control entre múltiples nodos. Sin embargo, una participación tan amplia también puede ralentizar el proceso de validación, ya que cuantos más nodos se involucren, más tiempo se requiere para alcanzar un consenso. En un escenario donde se deba gestionar un gran volumen de solicitudes esta ralentización podría generar diversos problemas operativos.

### **Más Descentralización, Menos Seguridad**

Depender de un gran número de nodos dentro de una red altamente descentralizada puede convertirse en un desafío de seguridad, ya que no existe un control central que supervise qué medidas se están aplicando. Esto hace más difícil prevenir y detectar ataques del tipo Sybil, en los que un actor malintencionado crea numerosos nodos con la intención de influir en el proceso de toma de decisiones o incluso intentar dominar partes de la red.

En cambio, en redes centralizadas resulta más sencillo imponer medidas de seguridad y responder rápidamente ante cualquier amenaza. Sin embargo, esta estructura también implica un riesgo al concentrar prácticamente todo el poder en una única entidad. Aunque ambos modelos presentan vulnerabilidades, el diseño de las blockchains actuales las hace prácticamente inmunes a ataques Sybil a gran escala, ya que sería necesario movilizar cientos de millones de activos para influir de forma significativa en sus decisiones.

Encontrar un equilibrio perfecto entre estas tres propiedades del trilema (escalabilidad, seguridad y descentralización) es una tarea compleja y, por el momento, no existe una solución definitiva. Esto ha motivado el desarrollo de distintos enfoques dentro del ecosistema blockchain, muchos de los cuales han producido avances prometedores. Un ejemplo es el sharding, un método que divide una blockchain en cadenas más pequeñas y especializadas que procesan segmentos concretos de datos, evitando que una única red tenga que gestionar todas las transacciones y operaciones.

Otro aspecto técnico relevante es la integración con los sistemas existentes. Muchas empresas exportadoras ya utilizan sus propios sistemas de gestión de la cadena de suministro, por lo que la capacidad de los smart contracts y de la tecnología blockchain para interactuar con estos entornos sin requerir una reconstrucción completa del sistema es clave para su adopción real.

Esto implica la necesidad de desarrollar interfaces y APIs capaces de comunicarse eficazmente con la blockchain, permitiendo un flujo de trabajo continuo que incorpore las funciones de los smart contracts en los procesos empresariales actuales sin generar interrupciones.

### **6.3. Viabilidad económica**

Valoraremos la viabilidad económica de la blockchain con un proyecto ficticio basado en la aplicación de esta tecnología a nivel europeo, lo llamaremos European Blockchain Trade Infrastructure (EBTI). Una propuesta destinada a dar apoyo a los servicios transfronterizos, centrándose en la gestión de la cadena de suministro y la autenticación de documentos.

#### **Costes de Implementación**

##### **Desarrollo e Infraestructura**

El desarrollo de la infraestructura sería lo más caro del proyecto y se estima que la creación de esta infraestructura podría costar entre 80 y 150 millones de euros. Este presupuesto incluye:

- **Adquisición de Hardware y Software:** 50 millones de euros para la compra de servidores y equipos necesarios para alojar la plataforma.
- **Desarrollo de la Plataforma:** 30 millones de euros para la creación de nodos distribuidos y la implementación de contratos inteligentes.
- **Integración con Sistemas Existentes:** 20 millones de euros para la integración con sistemas de las administraciones públicas y empresas privadas.

- **Pruebas Piloto:** 10 millones de euros para realizar pruebas piloto y asegurar que el sistema funcione correctamente antes de su lanzamiento completo.

### **Capacitación y Formación**

La formación del personal sería esencial para asegurar el uso y mantenimiento adecuados de la plataforma, así como contar con expertos procedentes de grandes proyectos. Los programas de capacitación y formación costarán aproximadamente 15 millones de euros, incluyendo:

- **Programas de Formación:** 10 millones de euros para organizar talleres y seminarios.
- **Desarrollo de Material Educativo:** 3 millones de euros para crear recursos de soporte y guías para los usuarios.
- **Soporte Técnico:** 2 millones de euros para asegurar que el personal esté bien preparado para utilizar la nueva tecnología y brindar asistencia.

### **Costes Administrativos y de Gestión**

La gestión y coordinación del proyecto implican la colaboración entre diversos países miembros y agencias de la UE. Así que contaremos con los siguientes gastos:

- **Equipo de Gestión de Proyectos:** 3 millones de euros anuales para supervisar la implementación.
- **Coordinación con Gobiernos Nacionales y Autoridades Locales:** 2 millones de euros anuales.
- **Evaluación Continua y Reporte:** 1 millón de euros anuales para monitorear el progreso del proyecto.

### **Beneficios para Empresarios, Transitarios y Agentes**

**Empresarios:** Aquellos empresarios que adopten este nuevo estándar podrán realizar un seguimiento completo de los productos, desde su fabricación hasta su entrega final. Esto permitirá disminuir los costes relacionados con la gestión de inventarios y fortalecer la relación con el cliente. Asimismo, la automatización de los procesos más complejos

contribuirá a reducir tanto el tiempo como los gastos vinculados al cumplimiento de normativas y regulaciones.

**Transitarios:** En el caso de los transitorios, la implementación del sistema favorecerá una mayor eficiencia operativa gracias a la reducción de la carga burocrática y la agilización de los trámites aduaneros. La EBTI facilitará una coordinación y comunicación más fluida entre todos los integrantes de la cadena logística, lo que se traducirá en una mayor puntualidad en las entregas.

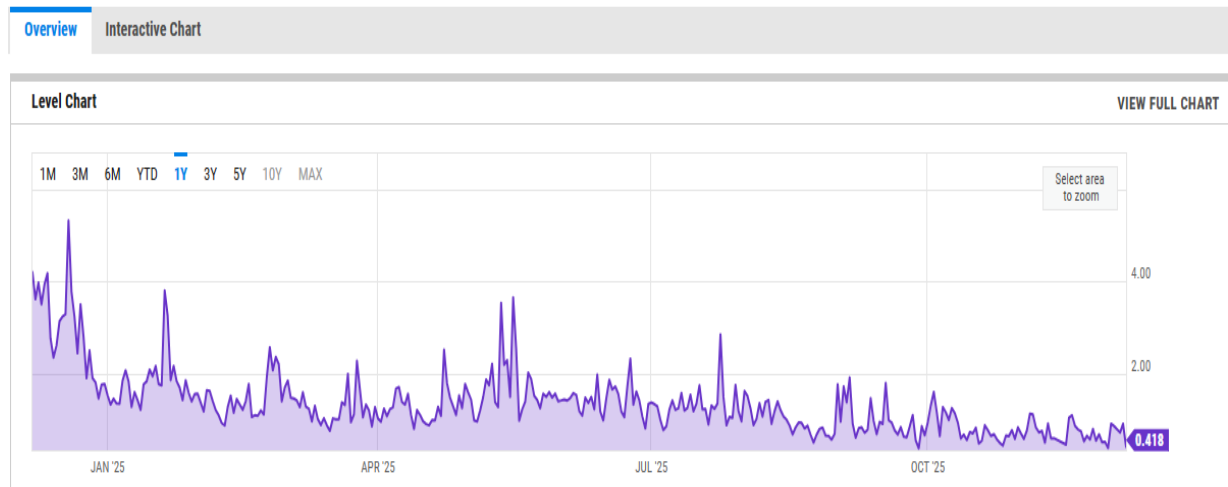
**Agentes:** Los agentes podrán aprovechar procesos más claros, menos susceptibles a errores y con un menor riesgo de fraude. La posibilidad de verificar la autenticidad de los documentos de forma rápida y segura también mejorará la eficiencia con la que desarrollan sus actividades.

Aunque la inversión inicial puede resultar elevada, los beneficios a largo plazo como la reducción de costes operativos, el aumento de la transparencia y la seguridad, y la simplificación del comercio internacional hacen que la implementación sea justificable. El retorno de la inversión debe evaluarse considerando el ahorro en trámites administrativos, la disminución del fraude, la mejora en la eficiencia operativa y el incremento del comercio transfronterizo.

Figura 7: Coste medio por transacción en distintas redes durante el 2025

### Bitcoin Average Transaction Fee (I:BATF)

0.4184 USD/tx for Dec 06 2025



Fuente: ycharts.com

## 6.4 Marco Legal de la UE para Blockchain y criptomonedas

Uno de los avances más relevantes dentro del ámbito regulatorio europeo es la aprobación del reglamento MiCA (*Boletín Oficial del Estado*, 2023). Fue adoptado por el Consejo de la UE en mayo de 2023 y establece un marco legal para la emisión y la prestación de servicios vinculados a las criptomonedas en toda la Unión Europea. El Reglamento MiCA establece un calendario de aplicación progresiva, con disposiciones que entran en aplicación por fases.

Al analizar directamente el documento oficial, se desprenden diversas perspectivas que permiten comprender hacia dónde avanza un marco regulatorio tan amplio y diverso, cuyo objetivo principal es precisamente garantizar un entorno seguro y transparente para los inversores. El marco legal incorpora definiciones claras para conceptos clave como criptoactivo, tokens de activos, tokens de dinero electrónico (e-money tokens) y proveedores de servicios de criptoactivos, lo que resulta fundamental para la correcta interpretación y aplicación de sus disposiciones.

Uno de los puntos fundamentales es la transparencia, ya que se exige que los emisores de criptomonedas faciliten a los inversores información clara y detallada, incluyendo documentos técnicos que describan su naturaleza y todos los riesgos implicados. Además, esta normativa otorga a las autoridades nacionales y a la Autoridad Europea de Valores y Mercados (ESMA) la capacidad de supervisar y controlar las actividades de los usuarios, así como de imponer sanciones y aplicar medidas correctivas para asegurar el cumplimiento del reglamento.

En lo referente a los intercambios de criptomonedas, se requiere que adopten políticas y procedimientos sólidos de gestión de riesgos, incorporando medidas de seguridad para proteger los activos de los clientes y evitar actividades fraudulentas. Por último, se fija un calendario preciso para su implementación y aplicación. Las disposiciones principales se activarán de manera progresiva, permitiendo que los emisores y los proveedores de servicios de criptoactivos se ajusten a las nuevas obligaciones, hasta quedar plenamente aplicable tras un periodo de implementación progresiva.

### **Cumplimiento de las Normativas de Protección de Datos**

Por otro lado, también encontramos el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, un elemento de gran relevancia debido a las estrictas condiciones que establece respecto a la recopilación, el almacenamiento y el tratamiento de datos personales. Los smart contracts que operan sobre blockchain y gestionan información personal de ciudadanos de la UE deben asegurar el cumplimiento del GDPR, lo que implica garantizar que dichos datos se procesen de forma legal, transparente y segura.

El carácter inmutable de la blockchain, como hemos mencionado en varias ocasiones a lo largo de este documento, supone un desafío para cumplir con el “derecho al olvido” recogido en el GDPR, el cual permite a los individuos solicitar la eliminación de sus datos personales. Este aspecto requerirá análisis y reflexión para poder encontrar soluciones que permitan alinear completamente esta tecnología con la normativa vigente.

## 7. CONCLUSIÓN

Este Trabajo de Fin de Grado ha analizado la evolución del dinero en el contexto de la digitalización y el impacto de la tecnología blockchain y los criptoactivos en el ecosistema financiero, combinando una perspectiva conceptual, técnica y regulatoria. A lo largo del trabajo se ha evidenciado que la transformación digital no solo afecta a los instrumentos de pago, sino también a la forma en que se diseñan, verifican y ejecutan las transacciones económicas, introduciendo nuevos modelos de intermediación, custodia y gobernanza.

Desde el punto de vista tecnológico, blockchain aporta ventajas relevantes —principalmente trazabilidad, integridad y resistencia a la manipulación—, pero también presenta límites estructurales asociados a la escalabilidad, la eficiencia y la sostenibilidad, así como riesgos operativos y de seguridad. En paralelo, los criptoactivos han demostrado capacidad para impulsar innovación financiera, pero su adopción generalizada se enfrenta a obstáculos significativos: volatilidad, asimetrías de información, riesgo de fraude, complejidad técnica y falta de madurez en determinados casos de uso. Por ello, su papel actual se sitúa entre la innovación con potencial transformador y la necesidad de control y protección del usuario para evitar externalidades negativas.

En el ámbito normativo, el marco europeo (con especial atención al Reglamento MiCA) representa un paso relevante hacia la homogeneización regulatoria, al buscar equilibrar innovación y seguridad jurídica, con mecanismos de supervisión y requisitos para emisores y proveedores de servicios. En consecuencia, la regulación se consolida como un factor decisivo para la confianza del mercado y la protección del consumidor, pero también como un elemento que condicionará la velocidad y la dirección de la adopción tecnológica en los próximos años.

## **Criterios y trazabilidad de la información**

Las conclusiones de este TFG se sustentan en una revisión documental seleccionada mediante criterios explícitos de calidad y pertinencia. En primer lugar, se priorizaron fuentes oficiales e institucionales (organismos de la Unión Europea y repositorios normativos, autoridades supervisoras, bancos centrales y organismos internacionales), por ser las referencias más adecuadas para conceptos monetarios, estabilidad financiera, marco legal y líneas de actuación pública. En segundo lugar, se incorporaron fuentes académicas y técnicas para fundamentar los aspectos de funcionamiento de blockchain, mecanismos de consenso y desafíos tecnológicos. Por último, se utilizaron fuentes generales y divulgativas únicamente como apoyo expositivo para clarificar conceptos, ejemplos y terminología, evitando que sustituyeran a la evidencia institucional o académica cuando se trataba de afirmaciones regulatorias o conclusiones críticas. La inclusión de fuentes respondió a criterios de autoría identificable, coherencia con el objeto de estudio, relevancia y contraste; y se excluyeron contenidos promocionales o no verificables.

## **Conclusiones según el tipo de lector (para quién va este TFG)**

### **Regulador y sector público:**

Aporta una síntesis de los riesgos y oportunidades que deben equilibrarse en el marco normativo (protección del consumidor, prevención del fraude, estabilidad financiera e impulso de la innovación), destacando el papel de marcos homogéneos como MiCA.

### **Sector financiero (banca, fintech y proveedores de servicios):**

Resume impactos y decisiones clave para la adopción: potencial en eficiencia y nuevos servicios, pero condicionado por escalabilidad, custodia, ciberseguridad y cumplimiento regulatorio.

### **Empresas no financieras y gestión (operaciones, logística, administración):**

Identifica casos de uso con valor (trazabilidad, verificación documental y automatización en escenarios adecuados) y limita expectativas señalando barreras reales (coste, interoperabilidad y madurez tecnológica).

### **Usuarios e inversores minoristas:**

Proporciona criterios básicos para interpretar riesgos frecuentes (volatilidad, irreversibilidad y estafas), reforzando la necesidad de educación financiera y prudencia.

### **Ámbito académico:**

Ofrece un marco integrado (tecnología–economía–regulación) y deja abiertas líneas futuras de estudio: efecto de la regulación en la adopción, análisis comparado por jurisdicciones y evaluación coste–beneficio de casos de uso.

En síntesis, la aportación principal del trabajo consiste en presentar una comprensión integrada del fenómeno (tecnología, economía y regulación) evitando tanto la idealización como el rechazo simplista. La conclusión final es que blockchain y los criptoactivos constituyen una innovación relevante, pero su consolidación depende de condiciones técnicas (escalabilidad y seguridad), económicas (utilidad real y eficiencia) y normativas (seguridad jurídica y protección efectiva del usuario). Por ello, el valor de estas tecnologías se materializa cuando se aplican con criterios de necesidad, proporcionalidad y supervisión, y no únicamente por tendencia o expectativa especulativa.

## 8. BIBLIOGRAFÍA

Banco Central Europeo. (n. d.). *Monetary aggregates. European Central Bank*. Recuperado de:

[https://www.ecb.europa.eu/stats/money\\_credit\\_banking/monetary\\_aggregates/html/index.en.html](https://www.ecb.europa.eu/stats/money_credit_banking/monetary_aggregates/html/index.en.html)

Bank for International Settlements. (n. d.). *BIS Innovation Hub work on central bank digital currency*. Recuperado de:

<https://www.bis.org/about/bisih/topics/cbdc.htm>

BeInCrypto. (n. d.). *Bitcoin y Ethereum: ataques del 51%*. Recuperado de:

<https://es.beincrypto.com/bitcoin-ethereum-objetivos-poco-probables-51-porciento/>

Binance Academy. (n. d.). *Cryptography glossary*. Recuperado de:

<https://www.binance.com/es/academy/glossary/cryptography>

Binance Academy. (n. d.). *Proof of Work vs Proof of Stake*. Recuperado de:

<https://www.binance.com/es/academy/articles/proof-of-work-vs-proof-of-stake>

Binance Academy. (n. d.). *What is blockchain and how does it work?* Recuperado de:

<https://www.binance.com/es/academy/articles/what-is-blockchain-and-how-does-it-work>

Binance Academy. (n. d.). *What is the blockchain trilemma?* Recuperado de:

<https://www.binance.com/es/academy/articles/what-is-the-blockchain-trilemma>

Bitcoin.org. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Recuperado de:

<https://bitcoin.org/en/bitcoin-paper>

Blockchain.com. (n. d.). *Confirmed transactions per day*. Recuperado de:

<https://www.blockchain.com/charts/n-transactions>

Boletín Oficial del Estado. (2023). Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA) (DOUE L 150). Recuperado de:

<https://www.boe.es/doue/2023/150/L00040-00205.pdf>

BBVA. (n. d.). *¿Por qué varía tanto el precio de las criptomonedas?* Recuperado de:

<https://www.bbva.com/es/innovacion/por-que-varia-tanto-el-precio-de-las-criptomonedas/>

Ciudadanía – INCIBE. (n. d.). *Historia de las criptomonedas en un clic*. Recuperado de:

<https://www.incibe.es/ciudadania/campanas/criptomonedas/historia-criptomonedas>

Coinbase. (n. d.). *What is volatility?* Recuperado de:

<https://www.coinbase.com/es-es/learn/crypto-basics/what-is-volatility>

CoinSpeaker. (n. d.). *Crypto investor phishing scam*. Recuperado de:

<https://www.coinspeaker.com/crypto-investor-100k-phishing-scam/>

European Banking Authority. (n. d.). *The EBA's supervisory role under MiCA*. Recuperado de:

<https://www.esma.europa.eu/activities/direct-supervision-and-oversight/ebas-supervisory-role-under-mica>

European Securities and Markets Authority. (n. d.). *Markets in Crypto-Assets Regulation (MiCA)*. Recuperado de:

<https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

European Union. (2023). *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA)*. EUR-Lex. Recuperado de:

<https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>

EUR-Lex. (2023). *European crypto-assets regulation (MiCA) (summary)*.

Recuperado de:

<https://eur-lex.europa.eu/ES/legal-content/summary/european-crypto-assets-regulation-mica.html>

Financial Action Task Force. (n. d.). *Virtual assets*. Recuperado de:

<https://www.fatf-gafi.org/en/topics/virtual-assets.html>

ForoCoin Blog. (n. d.). *¿Qué es el sharding?* Recuperado de:

<https://blog.forocoin.net/que-es-el-sharding/>

Investopedia. (n. d.). *eCash definition*. Recuperado de:

<https://www.investopedia.com/terms/e/ecash.asp>

KPMG. (n. d.). *Insights on blockchain and digital assets*. Recuperado de:

<https://kpmg.com/xx/en/our-insights.html>

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Recuperado de:

<https://bitcoin.org/bitcoin.pdf>

NoticiasTrabajo (Huffington Post). (2024, 24 de abril). *Estas son las monedas que puedes vender por miles de euros en el mercado numismático*. Recuperado de:

<https://noticiastrabajo.huffingtonpost.es/sociedad/monedas-pueden-alcanzar-miles-euros-mercado-numismatico-no-enganen/>

Novaluz. (n. d.). *Minería de criptomonedas y medio ambiente*. Recuperado de:

<https://novaluz.es/mineria-criptomonedas-y-medio-ambiente/>

Techopedia. (n. d.). *Techopedia*. Recuperado de:

<https://www.techopedia.com/>

The Objective. (2024, 21 de mayo). *Estafas por correos y mensajes fraudulentos*. Recuperado de:

<https://theobjective.com/sociedad/2024-05-21/estafas-correos-mensajes-fraudulentos-datos/>

TradingView. (n. d.). *BVOL – Bitcoin Historical Volatility Index*. Recuperado de:

<https://www.tradingview.com/symbols/BVOL/>

elDiario.es. (n.d.)

<https://www.eldiario.es/>

YCharts. (n.d.).

<https://ycharts.com/>

