



Facultad de Ciencias Económicas y Empresariales
ICADE

DE LA DESCENTRALIZACIÓN A LA REGULACIÓN: ¿SIGUEN SIENDO LAS CRIPTOMONEDAS UN PROYECTO DE LIBERTAD ECONÓMICA?

Autor: Santiago Núñez Clavijo
Director: Diego Villafáñez Sagardoy

MADRID | junio de 2026

Resumen:

En 2008, mientras el sistema financiero atravesaba uno de sus mayores colapsos, apareció Bitcoin con una propuesta radical: transferir valor entre personas sin intermediarios, sin bancos y sin posibilidad de censura. Más de quince años después, ese activo que nació para esquivar al sistema financiero se compra y se vende, en su mayor parte, a través de ese mismo sistema. Este trabajo analiza esa transformación con el objetivo de evaluar si las criptomonedas mantienen el carácter de proyecto de libertad económica que las dio origen o si se han convertido en un activo financiero más dentro del sistema regulado. La investigación recorre cinco dimensiones: los fundamentos tecnológicos y económicos de Bitcoin y su propuesta de desintermediación; la transformación del ecosistema con la aparición de Ethereum, las finanzas descentralizadas y la entrada de inversores institucionales; los riesgos financieros sistémicos derivados de esa evolución, ilustrados con los colapsos de Terra-Luna y FTX; la respuesta regulatoria internacional, con especial atención al Reglamento MiCA europeo y la fragmentación regulatoria estadounidense; y la tensión entre el ideal descentralizador original y la realidad de un mercado progresivamente institucionalizado. La hipótesis defendida es que la transformación ha sido real y profunda, pero no completa. El protocolo de Bitcoin conserva las propiedades técnicas que lo hacían atractivo como herramienta de libertad económica, y en ciertos contextos esas propiedades siguen siendo relevantes. Sin embargo, el ecosistema construido a su alrededor ha reproducido buena parte de las dinámicas de concentración, intermediación y supervisión que el proyecto quería evitar. La respuesta no es única: depende de qué parte del ecosistema se observe y de qué tipo de usuario se considere.

Palabras clave: criptoactivos, descentralización, Bitcoin, regulación financiera, finanzas descentralizadas, institucionalización, MiCA

Abstract:

In 2008, as the financial system was experiencing one of its worst crises, Bitcoin emerged with a radical proposal: to transfer value between individuals without intermediaries, without banks and without the possibility of censorship. More than fifteen years later, that asset born to bypass the financial system is bought and sold, for the most part, through that very system. This paper analyses that transformation with the aim of evaluating whether cryptocurrencies retain the character of an economic freedom project or have become just another financial asset within the regulated system. The research covers five dimensions: the technological and economic foundations of Bitcoin and its disintermediation proposal; the transformation of the ecosystem with the rise of Ethereum, decentralised finance and the entry of institutional investors; the systemic financial risks derived from that evolution, illustrated by the Terra-Luna and FTX collapses; the international regulatory response, with particular attention to the European MiCA Regulation and US regulatory fragmentation; and finally, the tension between the original decentralising ideal and the reality of a progressively institutionalised market. The hypothesis put forward is that the transformation has been real and profound, but not complete. The Bitcoin protocol retains the technical properties that made it attractive as a tool for economic freedom, and in certain contexts those properties remain relevant. However, the ecosystem built around it has reproduced many of the dynamics of concentration, intermediation and supervision that the project sought to avoid. The answer is not unique: it depends on which part of the ecosystem is examined and which type of user is considered.

Keywords: crypto-assets, decentralisation, Bitcoin, financial regulation, decentralised finance, institutionalisation, MiCA.

ÍNDICE

<i>Introducción y planteamiento de la investigación</i>	5
Introducción.....	5
Justificación y relevancia	5
Pregunta de investigación e hipótesis	5
Metodología.....	6
Estructura del trabajo.....	6
<i>Capítulo 1: Orígenes y Fundamentos del Proyecto Cripto</i>	7
1.1 El contexto de 2008: crisis financiera y desconfianza	7
1.2 Bitcoin y la idea de libertad económica	7
1.3 La tecnología blockchain y el modelo descentralizado	8
<i>Capítulo 2: Evolución económica y transformación del ecosistema</i>	10
2.1 De Bitcoin a Ethereum: del modelo entre pares a la aparición de nuevas funciones y servicios financieros descentralizados	10
2.2 Transformación del funcionamiento económico: de la minería hacia modelos basados en staking, liquidez y gobernanza	11
2.3 Entrada de inversores institucionales y transición hacia un mercado supervisado.....	12
<i>Capítulo 3: Riesgos y desafíos financieros</i>	14
3.1 Creciente interconexión entre el mercado cripto y el sistema financiero tradicional	14
3.2 Riesgos sistémicos: volatilidad, liquidez, concentración y contagio	15
3.3 Terra-Luna y FTX: dos tipos de fallo distintos.....	15
3.4 La reacción de los organismos internacionales.....	16
<i>Capítulo 4: La respuesta regulatoria</i>	18
4.1 El enfoque internacional: FSB, FMI y BIS	18
4.2 Europa: el Reglamento MiCA, DORA y el régimen DLT.....	18
4.3 Estados Unidos y la fragmentación regulatoria.....	19
4.4 Efectos sobre los inversores y el mercado	20
<i>Capítulo 5: ¿Siguen siendo un proyecto de libertad económica?</i>	22
5.1 La paradoja de la descentralización: concentración de poder en un sistema que prometía eliminarlo	22
5.2 La transformación de la demanda: del usuario ideológico al inversor institucional	23
5.3 Innovación, regulación y poder de mercado: ¿puede existir libertad económica real en un mercado institucionalizado?	24
<i>Conclusiones</i>	25
Síntesis de los hallazgos.....	25
Evaluación de la hipótesis.....	25
Reflexiones finales	26

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado 27

Bibliografía 28

Introducción y planteamiento de la investigación

Introducción

En octubre de 2008, mientras la crisis financiera arrasaba con la confianza en los bancos, apareció en una lista de correo un documento de nueve páginas firmado por un tal Satoshi Nakamoto. Nadie sabía quién era, y todavía no se sabe. Lo que proponía sonaba a ciencia ficción: que dos personas pudieran mandarse dinero directamente, sin un banco que lo procesara, sin una cámara de compensación que lo liquidara y sin ninguna autoridad que pudiera bloquearlo. El momento no era casual. La crisis acababa de enseñar lo frágil que era el sistema, y Bitcoin se presentaba como algo que no obligaba a fiarse de nadie.

Hoy cuesta reconocer aquel proyecto en lo que las criptomonedas se han convertido. Bitcoin mueve billones de dólares y entre sus mayores tenedores están los gestores de activos más grandes del mundo. BlackRock vende ETF de bitcoin, hay empresas cotizadas que lo guardan en su tesorería y medio planeta tiene ya normativa específica para el sector. El activo que nació para esquivar a los intermediarios se compra y se vende, sobre todo, a través de esos mismos intermediarios.

De ahí la pregunta que recorre este trabajo: ¿siguen siendo las criptomonedas un proyecto de libertad económica, o son ya un activo financiero más dentro del sistema regulado que querían sustituir?

Justificación y relevancia

Estudiar esta cuestión tiene sentido por varios motivos. El mercado de criptoactivos ha alcanzado un tamaño y una interconexión con el sistema financiero tradicional que lo convierten en un asunto de estabilidad financiera, no solo de curiosidad tecnológica. Pero más allá de su magnitud, el caso es interesante en sí mismo: la tensión entre el ideal descentralizador de los inicios y la realidad de un mercado cada vez más institucionalizado funciona como un laboratorio para entender cómo evolucionan las innovaciones financieras cuando se topan con las estructuras existentes. Y los últimos años han sido especialmente ricos en material para ese análisis, del colapso de Terra-Luna y FTX a la aprobación de los ETF de bitcoin.

Pregunta de investigación e hipótesis

La pregunta ya está sobre la mesa: si las criptomonedas conservan ese carácter de proyecto de libertad económica que tuvieron al nacer, o si la evolución tecnológica, económica y regulatoria las ha terminado convirtiendo en un activo financiero más del sistema convencional.

Lo que aquí se defiende es que la transformación ha sido real y profunda, aunque no completa. El protocolo de Bitcoin no ha perdido las propiedades técnicas que lo hacían atractivo como herramienta de libertad económica, y en según qué contextos esas propiedades pesan. Lo que ha cambiado es todo lo demás: el ecosistema levantado a su alrededor ha acabado reproduciendo buena parte de la concentración, la intermediación y la supervisión que el proyecto quería dejar atrás. De ahí que no haya una respuesta única. Depende de qué parte del ecosistema se mire y de qué usuario se tenga delante.

Metodología

El enfoque es cualitativo y analítico-descriptivo. Se apoya en la revisión de literatura académica y documentos institucionales, y compara la etapa inicial del ecosistema con su configuración actual. Entre las fuentes hay literatura sobre economía monetaria y blockchain, informes del BIS, el FMI y el FSB, y normativa oficial como MiCA. No hay trabajo empírico con datos cuantitativos propios, aunque sí se usan estadísticas de fuentes especializadas a modo de apoyo.

Estructura del trabajo

Son cinco capítulos. El primero sitúa el nacimiento de Bitcoin en la crisis de 2008 y desgrana los principios de libertad económica y descentralización que lo inspiraron. El segundo va siguiendo cómo evolucionó el ecosistema: el salto de Bitcoin a Ethereum, la aparición de DeFi y la entrada del dinero institucional. El tercero se ocupa de los riesgos financieros que llegaron con esa evolución, usando Terra-Luna y FTX como casos de estudio. El cuarto entra en la respuesta de los reguladores, sobre todo MiCA en Europa frente al desorden competencial estadounidense. Y el quinto vuelve a la pregunta del principio para responderla con todo lo anterior ya sobre la mesa.

Capítulo 1: Orígenes y Fundamentos del Proyecto Cripto

1.1 El contexto de 2008: crisis financiera y desconfianza

Para entender Bitcoin hay que volver a 2008. Ese año el sistema financiero moderno sufrió uno de sus mayores colapsos, y con él se vino abajo la confianza en la estabilidad, la transparencia y la legitimidad de los intermediarios financieros. Bitcoin nace en ese momento, y no se entiende fuera de él.

¿De dónde venía la crisis? Del estallido de la burbuja inmobiliaria estadounidense y del uso masivo de productos financieros atados a hipotecas de mala calidad (Brunnermeier, 2009). Los bancos estaban entrelazados entre sí y muy endeudados, así que cuando empezaron los impagos el contagio fue rápido por todo el sistema internacional. Ante el riesgo de un colapso generalizado, los Estados tuvieron que intervenir de urgencia (Gorton, 2010).

Esas intervenciones fueron, en su mayoría, rescates públicos a bancos y grandes entidades. Y abrieron un debate que todavía colea. Se socializaron las pérdidas de instituciones privadas que habían asumido riesgos enormes, y al hacerlo se mandó un mensaje difícil de borrar: el sistema financiero estaba protegido por el poder público pasara lo que pasara. Los economistas lo llaman moral hazard. Si el Estado acaba cubriendo las pérdidas, ¿qué incentivo queda para gestionar el riesgo con cabeza? (Acharya et al., 2009).

La factura fue una desconfianza que fue mucho más allá de los bancos. Alcanzó a la propia arquitectura del sistema monetario (Reinhart & Rogoff, 2009). El sistema se empezó a ver como algo opaco, injusto y demasiado concentrado en pocas manos, capaces de influir en decisiones políticas y económicas que afectaban a todos. Los bancos centrales, los reguladores, las instituciones encargadas de la estabilidad financiera: nadie salió indemne (Gorton, 2010).

Ahí es donde cobran sentido las propuestas de sistemas alternativos. Menos dependencia de intermediarios, más reglas claras y verificables. Bitcoin aparece en ese hueco: un sistema de dinero electrónico entre pares que quería eliminar la necesidad de confiar en instituciones centrales y sustituirla por mecanismos técnicos y criptográficos (Nakamoto, 2008). Sus principios de descentralización y libertad económica no fueron un capricho tecnológico. Fueron una respuesta a lo que 2008 había dejado al descubierto (Reinhart & Rogoff, 2009).

1.2 Bitcoin y la idea de libertad económica

La confianza en bancos e instituciones estaba por los suelos cuando Satoshi Nakamoto publicó su propuesta en 2008: un sistema de dinero electrónico entre pares (peer-to-peer electronic cash system) que permitía transferir valor de forma directa, sin intermediarios de ningún tipo (Nakamoto, 2008).

La apuesta de fondo es prescindir de la confianza en terceros, lo que se conoce como sistema trustless. El dinero tradicional necesita bancos, cámaras de compensación e instituciones varias para que un pago llegue de A a B. Bitcoin lo resuelve con reglas técnicas y criptográficas que validan las transacciones solas (Nakamoto, 2008; Böhme et al., 2015). El término puede despistar: trustless no significa ausencia de confianza, sino que esa confianza ya no recae en instituciones humanas sino en protocolos matemáticos que cualquiera puede verificar (Narayanan et al., 2016). Es un desplazamiento, no una eliminación.

Desde ahí, Bitcoin se puede leer como un proyecto de libertad económica. Cada usuario controla sus fondos sin depender de una autoridad central, sin pedir permiso y sin riesgo de censura. En el sistema tradicional el acceso está condicionado por regulaciones y decisiones de terceros; aquí no (Böhme et al., 2015).

La política monetaria también es distinta. La emisión de bitcoin tiene un techo fijo de 21 millones de unidades y sigue un calendario predeterminado que nadie puede alterar (Nakamoto, 2008). Sus defensores ven en eso un argumento de soberanía individual y protección frente a la expansión monetaria discrecional (Böhme et al., 2015). Pero reducirlo a ideología sería simplificar. Detrás hay también una motivación práctica muy concreta: un sistema de pagos global y accesible que resulta especialmente útil para quien está excluido de la banca o desconfía de sus intermediarios (Narayanan et al., 2016).

Aun así, esa promesa de descentralización absoluta hay que tomarla con matices. Desde el principio, el funcionamiento de la red dependía de dinámicas económicas y técnicas que ya condicionaban cómo se repartía el poder dentro del sistema (Böhme et al., 2015).

Lo que Bitcoin propone, en el fondo, es una innovación tecnológica con una crítica implícita al sistema financiero metida dentro. Desintermediación, control individual y reglas transparentes: ese es el corazón del ideal cripto original. Un ideal que, como iremos viendo, acabará chocando con la evolución del mercado, la entrada de nuevos actores y la llegada de la regulación.

1.3 La tecnología blockchain y el modelo descentralizado

Bitcoin no es solo una innovación monetaria. También es, y sobre todo, una innovación tecnológica. Lo que lo hace funcionar es la blockchain: un sistema de registro distribuido que almacena y verifica transacciones sin que haga falta una autoridad central (Nakamoto, 2008).

¿Qué es una blockchain? En esencia, un libro contable digital compartido entre los participantes de una red. En vez de un registro único en manos de una institución, como en la banca, la información se copia en muchos nodos a la vez. Las transacciones se agrupan en bloques, y cada bloque se enlaza criptográficamente con el anterior, formando una cadena cronológica. Gracias a ese encadenamiento, modificar un dato ya confirmado se vuelve casi imposible. De ahí la propiedad que define al sistema: la inmutabilidad (Narayanan et al., 2016).

Aquí entra el modelo descentralizado de validación. En el sistema de siempre, comprobar que un pago es legítimo es tarea de entidades centrales. Bitcoin lo resuelve de otra manera: con un mecanismo de consenso distribuido en el que los participantes de la red acuerdan qué transacciones son válidas siguiendo reglas predefinidas (Böhme et al., 2015). Así la confianza deja de depender de una institución concreta y pasa a apoyarse en el propio protocolo.

Que la red sea descentralizada significa que nadie controla el sistema entero. Cualquiera puede entrar descargando el software y conectándose, lo que refuerza esa imagen de apertura y neutralidad. Ahora bien, hay que entender la descentralización en clave económica y técnica: la red se mantiene gracias a incentivos pensados para premiar el comportamiento honesto de quienes la validan y la aseguran (Böhme et al., 2015).

La blockchain es, en suma, el andamiaje que sostiene el ideal de desintermediación del proyecto cripto original. Al sustituir la autoridad central por reglas compartidas y verificables,

monta un modelo que busca juntar transparencia, seguridad y autonomía individual. Pero esa descentralización inicial, como se verá en los capítulos siguientes, se ve matizada por la evolución del ecosistema y por una profesionalización del mercado que introduce dinámicas nuevas.

Capítulo 2: Evolución económica y transformación del ecosistema

2.1 De Bitcoin a Ethereum: del modelo entre pares a la aparición de nuevas funciones y servicios financieros descentralizados

Esa tensión entre el ideal original y la realidad del ecosistema empieza a manifestarse precisamente en la evolución tecnológica y económica que se analiza en este capítulo. Bitcoin demostró que era posible transferir valor entre dos personas sin un banco entre medias, lo que suponía una ruptura relevante respecto al modelo financiero tradicional. Pero el protocolo tenía un límite evidente: estaba diseñado para mover bitcoins de un punto a otro, y poco más. Implementar cualquier lógica más compleja sobre él era, en la práctica, muy difícil.

Es en ese contexto donde surge Ethereum. En 2013, Vitalik Buterin publicó su *whitepaper* con una propuesta distinta: una blockchain de propósito general capaz de ejecutar programas arbitrarios (*Buterin, 2013*). El concepto central era el *smart contract*, un código almacenado en la cadena que se ejecuta automáticamente cuando se cumplen las condiciones programadas, sin que ninguna de las partes tenga que confiar en la otra ni recurrir a un árbitro externo (*Narayanan et al., 2016*). La red entró en funcionamiento en 2015.

La diferencia técnica con Bitcoin tiene consecuencias económicas concretas. Bitcoin opera con un modelo UTXO: cada transacción consume outputs de transacciones anteriores no gastados y genera outputs nuevos. Es transparente, pero la lógica programable es muy limitada. A diferencia del modelo UTXO de Bitcoin, Ethereum lleva la contabilidad por cuentas: cada dirección tiene un saldo que se actualiza transacción a transacción y puede llamar a contratos que ejecutan su propia lógica (*Wood, 2014*). El entorno que hace posible esa ejecución es la Ethereum Virtual Machine (EVM), que corre el mismo código en todos los nodos de la red a la vez.

Sobre esa base se fueron añadiendo capas. El estándar ERC-20, de 2015, permitió crear tokens fungibles con una interfaz común: desde utility tokens que dan acceso a un servicio hasta governance tokens con derechos de voto (*Buterin, 2013*). En 2017 llegó el ERC-721 para los NFT, activos únicos no intercambiables entre sí. Cada estándar nuevo abría posibilidades que el anterior no tenía.

De ahí nació DeFi. La idea era ofrecer préstamos, intercambios y derivados sin custodios centrales, con los usuarios manteniendo el control de sus fondos en todo momento (*BIS, 2021*). El mecanismo básico son los pools de liquidez: masas comunes de criptoactivos gestionadas por contratos inteligentes que actúan como contrapartes automáticas. Quien aporta activos al pool recibe una parte de las comisiones; quien los necesita, paga.

Entre 2018 y 2021 surgieron los protocolos que hoy definen el espacio. Uniswap introdujo el modelo de creador de mercado automatizado (AMM): el precio entre dos tokens no lo fija un libro de órdenes con compradores y vendedores, sino una función matemática que mantiene constante el producto de las reservas de ambos (*Adams et al., 2021*). Compound y Aave construyeron mercados de préstamos donde los tipos de interés se ajustan automáticamente según la utilización de los pools. Synthetix ofreció contratos derivados sobre activos reales (divisas, materias primas, índices) sin necesidad de acceder a ningún mercado regulado.

Lo que hace peculiar a toda esta arquitectura es la composabilidad. Los protocolos DeFi pueden interactuar entre sí dentro de una misma transacción: un usuario puede pedir prestado un activo

en Aave, cambiarlo en Uniswap, depositarlo como colateral en otro protocolo y retirar liquidez de un cuarto, todo en un único bloque y sin intervención humana. De ahí nacen los compuestos DeFi: agregadores de DEX, yield aggregators y flash loans que encadenan operaciones de una complejidad que habría sido impensable hace quince años.

La transición de Bitcoin a Ethereum fue, antes que nada, un cambio de pregunta. Bitcoin preguntaba cómo mover valor sin intermediarios. Ethereum preguntaba qué más se podía hacer con una red que ejecuta código de forma descentralizada. Esa segunda pregunta es la que explica por qué la mayor parte de la innovación financiera del ecosistema cripto de la última década se ha construido sobre Ethereum, y no sobre Bitcoin.

2.2 Transformación del funcionamiento económico: de la minería hacia modelos basados en staking, liquidez y gobernanza

El mecanismo con el que Bitcoin asegura su red tiene un coste deliberado. Para añadir un bloque, los mineros deben resolver un problema computacional que consume cantidades importantes de electricidad. Ese coste es lo que hace que atacar la red sea económicamente inviable: habría que superar el poder de cómputo acumulado de toda la red honesta, que en el caso de Bitcoin representa un gasto energético comparable al de países como Bélgica o Noruega (*Narayanan et al., 2016*). Quien lo resuelve primero recibe una recompensa en bitcoins recién emitidos más las comisiones de las transacciones del bloque.

La política monetaria de Bitcoin está integrada en el protocolo. Cada 210.000 bloques, aproximadamente cada cuatro años, la recompensa por bloque se reduce a la mitad, el halving. El cuarto ocurrió en abril de 2024, dejando la recompensa en 3,125 BTC por bloque. El total nunca superará los 21 millones (*Nakamoto, 2008*). Esto elimina la posibilidad de que nadie altere la oferta de forma discrecional, que era precisamente uno de los reproches al sistema financiero tradicional tras 2008. Sin embargo, genera una pregunta incómoda a largo plazo: cuando la recompensa por bloque sea insignificante, ¿serán suficientes las comisiones de transacción para mantener el incentivo a los mineros? Es un debate abierto y sin respuesta clara (*Budish, 2018*).

Ethereum tomó un camino distinto. En septiembre de 2022, completó la transición conocida como The Merge: sustituyó la prueba de trabajo por la prueba de participación (Proof of Stake). En este sistema, quienes quieren validar bloques no compiten mediante cómputo, sino que depositan ether como garantía (el mínimo son 32 ETH) y el protocolo los selecciona aleatoriamente para proponer y atestar bloques. Si un validador actúa de forma deshonesto, puede perder parte o la totalidad del depósito, el llamado slashing (*Buterin et al., 2022*). El consumo energético de Ethereum cayó más de un 99%. Pero surgieron otros problemas: quienes tienen más capital tienen más probabilidad de ser seleccionados, lo que tiende a concentrar el poder de validación.

Para resolver la barrera de los 32 ETH, aparecieron protocolos de staking líquido como Lido Finance. La mecánica es simple: el usuario delega su ether en validadores profesionales y recibe a cambio un token llamado stETH, que representa el depósito más los intereses acumulados, y que puede usar en otros protocolos DeFi. El problema es que Lido ha llegado a concentrar más del 30% del total de ETH en staking (*DefiLlama, 2024*), lo que lo convierte en el protocolo dominante de la red y genera riesgos que la propia literatura académica reconoce, incluyendo la posibilidad de que sus smart contracts actúen como un punto único de fallo para

toda la red Ethereum (*Heimbach et al., 2023*). Es una solución que funciona individualmente pero que, a escala, reproduce el problema de concentración que el PoS pretendía corregir.

La provisión de liquidez en protocolos DeFi añade otra capa. Quien deposita activos en un pool de Uniswap o Curve recibe una fracción de las comisiones que pagan los traders. A eso se sumó el yield farming: los protocolos emiten sus propios tokens de gobernanza como incentivo adicional para atraer liquidez en sus primeras etapas. Durante el llamado DeFi Summer de 2020-2021, las rentabilidades anualizadas que ofrecían algunos protocolos eran de tres y cuatro dígitos. No duraron. Los incentivos en tokens inflacionarios atraen capital especulativo que se marcha en cuanto las recompensas caen, dejando pools vacíos y precios colapsados (*BIS, 2021*). El patrón se ha repetido suficientes veces como para que ya no sorprenda.

La gobernanza descentralizada cierra el cuadro. La mayoría de los protocolos DeFi con peso están gestionados por DAOs: estructuras donde las decisiones sobre cambios en parámetros de riesgo, distribución de ingresos y actualizaciones de código se toman por votación de los tenedores del token de gobernanza. En teoría, es la versión cripto de la democracia directa. En la práctica, los tokens de gobernanza suelen estar muy concentrados en equipos fundadores, fondos de capital riesgo y primeros inversores. Que el 1% de los tenedores de MKR, el token de MakerDAO, controle más de la mitad del poder de voto no es una anomalía, es un patrón recurrente (*Buterin et al., 2022*). La descentralización de la gobernanza, al menos tal como está implementada ahora, es más una aspiración que una realidad operativa.

El resultado de todo esto es un ecosistema cuya complejidad económica es radicalmente distinta a la de Bitcoin en 2009. El modelo actual, que combina staking, provisión de liquidez, yield farming y gobernanza tokenizada, requiere una sofisticación considerable para navegarlo sin perder dinero. Pero más allá de la complejidad, hay un patrón que merece atención: el ecosistema que nació con la promesa de eliminar la concentración de poder ha ido recreando nuevas formas de ella. Los pools de minería concentran el hashrate, los protocolos de staking líquido concentran el poder de validación, y los tokens de gobernanza concentran las decisiones en manos de unos pocos. Los actores son distintos a los del sistema financiero tradicional, pero la dinámica de concentración no lo es tanto. Esta tensión entre el ideal descentralizador original y la realidad del ecosistema actual es el hilo que se desarrollará con más profundidad en el Capítulo 5.

2.3 Entrada de inversores institucionales y transición hacia un mercado supervisado

Durante sus primeros años, el mercado cripto operó en gran medida al margen del sistema financiero convencional. Los participantes eran principalmente individuos (programadores, especuladores, gente ideológicamente comprometida con la idea) que usaban exchanges con escasos controles y sin acceso a los instrumentos que utilizan los inversores profesionales. Eso empezó a cambiar con la explosión de las ICOs en 2017, que atrajo a los primeros fondos de capital riesgo, y se aceleró de forma clara a partir de 2020.

La entrada institucional siguió varias vías simultáneas. La primera fue la aparición de vehículos regulados para obtener exposición a criptoactivos sin tener que custodiarlos directamente. El Grayscale Bitcoin Trust existía desde 2013, pero fue a partir de 2020 cuando empezó a tener una presencia significativa. El salto definitivo llegó en enero de 2024, cuando la SEC aprobó los primeros ETF de Bitcoin al contado en Estados Unidos, entre ellos los de BlackRock, Fidelity e Invesco (*FSB, 2024*). El ETF de BlackRock se convirtió en uno de los de mayor

crecimiento en la historia reciente de la industria de fondos, captando decenas de miles de millones de dólares en sus primeros meses. Eso no es capital minorista.

La segunda vía fue la incorporación de bitcoin en balances corporativos. MicroStrategy, con Michael Saylor al frente, empezó en 2020 a convertir su tesorería en bitcoin y acumuló más de 200.000 BTC a lo largo de los años siguientes. Tesla anunció en 2021 una inversión de 1.500 millones. Muchas empresas deshicieron luego sus posiciones, pero el debate sobre si bitcoin tiene cabida como reserva de valor en un balance corporativo quedó instalado.

La tercera vía fue la integración de infraestructuras cripto en el sistema financiero tradicional. Goldman Sachs, Morgan Stanley y JPMorgan comenzaron a ofrecer productos vinculados a criptoactivos a sus clientes institucionales. Visa y Mastercard acordaron liquidar transacciones en stablecoins. PayPal introdujo la compraventa de criptomonedas. La frontera entre el mundo cripto y el convencional se fue difuminando.

El mercado cripto que salió de todo esto tenía poco que ver con el de 2015. Los exchanges ya no eran foros de intercambio entre particulares: tenían departamentos de compliance, procedimientos KYC y AML, y equipos dedicados a gestionar la relación con los reguladores. Custodiar bitcoin pasó a ser un negocio especializado; Coinbase Custody, Fireblocks y BitGo crecieron para atender a fondos e instituciones que no podían o no querían gestionar sus propias claves privadas. Antes era raro auditar un smart contract. Pasó a ser obligatorio.

La presión regulatoria no llegó solo por el crecimiento del mercado, sino también por sus propios desastres. En mayo de 2022, Terra-Luna se derrumbó en cuestión de días. El mecanismo algorítmico que supuestamente mantenía el precio de UST estable dependía de la confianza en el token Luna; cuando esa confianza se rompió, ambos colapsaron en espiral y borraron más de 40.000 millones de dólares en valor de mercado (*FSB, 2022*). Seis meses después cayó FTX. La segunda mayor plataforma de intercambio del mundo resultó estar mezclando fondos de clientes con los propios, con una contabilidad opaca que ningún mecanismo de supervisión existente había detectado. Su colapso arrastró a varios prestamistas y fondos del sector.

Ambos episodios aceleraron el trabajo regulatorio. En Europa, el Reglamento MiCA, aprobado en 2023 y con plena aplicación desde finales de 2024, establece un marco armonizado para emisores de criptoactivos y proveedores de servicios, con requisitos de capital, transparencia, custodia y conducta de mercado. En Estados Unidos, la situación es más desordenada: la SEC y la CFTC disputan la jurisdicción sobre distintos tipos de activos, y varios emisores han sido objeto de procedimientos sancionadores sin que haya un marco federal claro que los respalde.

Lo que emerge de todo este proceso es un mercado que ha ganado escala y legitimidad institucional, pero a un coste que merece señalarse. La custodia de activos ha pasado de wallets individuales a grandes intermediarios. El acceso al mercado depende cada vez más de plataformas reguladas que deciden quién puede operar y en qué condiciones. El capital que mueve los precios no es el de usuarios ideológicamente comprometidos con la descentralización, sino el de fondos que buscan rentabilidad. Cada uno de estos cambios es comprensible por separado, pero su combinación plantea una pregunta incómoda: si el sistema resultante reproduce las mismas dinámicas de intermediación y concentración que Bitcoin pretendía sustituir, ¿en qué medida sigue siendo un proyecto de libertad económica? Es la pregunta que articula el resto de este trabajo.

Capítulo 3: Riesgos y desafíos financieros

3.1 Creciente interconexión entre el mercado cripto y el sistema financiero tradicional

La creciente integración institucional descrita en el capítulo anterior no es solo una transformación del mercado cripto en sí mismo. Tiene también consecuencias sobre el sistema financiero tradicional, porque a medida que ambos mundos se han ido conectando, los riesgos de uno han empezado a trasladarse al otro. Durante la mayor parte de la primera década de Bitcoin, la pregunta de si los criptoactivos podían desestabilizar el sistema financiero convencional tenía una respuesta fácil: no, porque los dos mundos apenas se rozaban. Bitcoin no aparecía en balances bancarios, no había productos derivados regulados sobre él y su capitalización era demasiado pequeña para importar a nivel sistémico. Eso cambió. No de golpe, sino poco a poco, y luego muy rápido.

El primer punto de contacto real fue la exposición institucional. Fondos de inversión alternativos empezaron a incluir criptoactivos en sus carteras, aparecieron productos estructurados referenciados a su precio y algunos bancos comenzaron a ofrecer servicios de custodia o trading a sus clientes institucionales. Silvergate Bank y Signature Bank son el ejemplo más concreto de lo que ocurre cuando esa exposición se vuelve demasiado concentrada: ambas entidades habían construido gran parte de su negocio sobre servicios al sector cripto y quebraron en marzo de 2023, parcialmente arrastradas por el impacto del colapso de FTX sobre sus clientes (*FSB, 2023*). Fue la primera vez que el contagio cripto se materializó directamente en el balance de bancos regulados y supervisados.

Las stablecoins añaden otra capa de conexión, más estructural. Tether (USDT) y USD Coin (USDC), las dos con mayor capitalización, mantienen sus reservas en activos del sistema financiero tradicional: depósitos bancarios, letras del Tesoro y papel comercial (*BIS, 2022*). Una salida masiva de stablecoins puede forzar liquidaciones de activos tradicionales. Pero la conexión funciona en ambas direcciones. Cuando Silicon Valley Bank quebró en marzo de 2023, USDC perdió temporalmente su paridad con el dólar porque Circle tenía reservas depositadas ahí. El episodio se resolvió en menos de 48 horas, pero dejó claro que la frontera entre ambos sistemas ya no funciona como cortafuegos.

Hay una tercera vía de exposición más difícil de rastrear: fondos de pensiones, aseguradoras y gestoras de patrimonio que han incorporado criptoactivos como activo alternativo en sus carteras. La magnitud varía según la jurisdicción, pero su existencia implica que una caída brusca del mercado cripto puede afectar a carteras de ahorro de inversores minoristas que ni saben que tienen esa exposición.

El FMI señaló en 2022 que la correlación entre los precios de los criptoactivos y la renta variable había aumentado de forma significativa, especialmente en periodos de estrés (*IMF, 2022*). En los primeros años de Bitcoin esa correlación era prácticamente inexistente. En las caídas de 2020 y 2022, bitcoin y los índices bursátiles bajaron juntos, respondiendo a las mismas tensiones macroeconómicas. Eso no es una coincidencia, es integración.

3.2 Riesgos sistémicos: volatilidad, liquidez, concentración y contagio

Bitcoin ha caído más de un 50% en cuestión de meses en repetidas ocasiones. El resto del mercado generalmente cae más. Esta volatilidad no es solo una característica incómoda del activo; tiene causas estructurales que la hacen persistente.

La más básica es la ausencia de un valor fundamental observable. Una acción tiene flujos de caja descontados. Un bono tiene un tipo de interés y un emisor con solvencia medible. Bitcoin no tiene nada equivalente: su precio depende de las expectativas sobre su adopción futura y de la disposición de los participantes a seguir manteniéndolo. Eso lo hace muy sensible al sentimiento del mercado (*Biais et al., 2023*). Cuando la narrativa cambia, el precio cambia con ella, y las narrativas en el mercado cripto pueden girar en cuestión de días.

La liquidez es otro problema. Ha crecido mucho, pero sigue siendo frágil comparada con la de los mercados de divisas o deuda soberana. En momentos de estrés, los libros de órdenes se vacían rápido y los movimientos de precio se amplifican. Parte de la liquidez aparente proviene de prácticas de market making poco transparentes en exchanges sin los estándares de los mercados regulados. Esa liquidez tiende a desaparecer exactamente cuando más se necesita (*Gandal et al., 2021*).

La concentración de la propiedad complica aún más el cuadro. Foley et al. (2019) estimaron que el 1% de las direcciones de bitcoin controlaba más del 27% del supply en circulación. Cuando esas posiciones se mueven, el mercado lo nota. Las transacciones de gran volumen de estas wallets pueden desplazar el precio por sí solas, en un mercado donde la línea entre movimiento orgánico y manipulación es muy difícil de trazar.

El contagio dentro del ecosistema tiene su propia lógica. La composabilidad de DeFi, que en el capítulo anterior describíamos como una de sus propiedades más innovadoras, es también lo que hace que los fallos se propaguen. Un protocolo que cae arrastra a los que dependían de él como fuente de liquidez o colateral. Cuando Terra-Luna colapsó en 2022, Three Arrows Capital, uno de los mayores fondos cripto del momento, quebró poco después por su exposición. Eso arrastró a Celsius, Voyager y BlockFi (*FSB, 2022*). La cadena entera tardó semanas en caer, pero fue inevitable desde el primer eslabón.

El BIS apunta que esta dinámica tiene similitudes con el contagio financiero tradicional, pero con una diferencia relevante: la transparencia on-chain hace que los problemas sean visibles antes de que una institución quiebre formalmente, lo que puede acelerar las retiradas de liquidez (*Cornelli et al., 2023*). En un sistema sin mecanismos de resolución ordenada, esa velocidad es más un riesgo que una ventaja.

3.3 Terra-Luna y FTX: dos tipos de fallo distintos

2022 fue el año en que el mercado cripto demostró que sus riesgos eran reales. Los dos grandes colapsos, Terra-Luna en mayo y FTX en noviembre, son casos de estudio útiles no porque sean similares, sino porque no lo son en absoluto. Cada uno ilustra un tipo de fallo diferente.

Terra-Luna fue un fallo de diseño. El ecosistema giraba en torno a dos tokens: UST, una stablecoin algorítmica sin respaldo en activos externos que pretendía mantener la paridad con el dólar, y Luna, el token nativo de la red. El mecanismo de estabilización dependía de un arbitraje circular: si UST bajaba de un dólar, los usuarios podían quemarlo a cambio de Luna

a precio nominal, reduciendo la oferta de UST y presionando su precio al alza. El problema es que ese mecanismo solo funciona mientras hay demanda de Luna. Cuando Anchor Protocol, que ofrecía rentabilidades del 20% anual sobre UST, empezó a sufrir retiradas masivas en mayo de 2022, se desencadenó la espiral. La caída de UST requería emitir más Luna para sostener el arbitraje, lo que diluía Luna, lo que erosionaba la confianza en UST, lo que generaba más retiradas. En menos de una semana Luna pasó de más de 80 dólares a prácticamente cero (*Briola et al., 2023*). Más de 40.000 millones de dólares en valor de mercado desaparecieron.

Lo más relevante para el análisis regulatorio no es el colapso en sí, sino que el riesgo era identificable antes de que ocurriera. La fragilidad de un sistema de estabilización basado en confianza circular sin respaldo real había sido señalada por analistas e incluso por el propio BIS con anterioridad. Pero sin supervisión prudencial, identificar un riesgo no activa ningún mecanismo de corrección.

FTX es otra historia. No fue un fallo de diseño sino fraude directo. FTX era el segundo mayor exchange centralizado del mundo, con millones de usuarios y una valoración que superó los 30.000 millones de dólares en su pico. En noviembre de 2022, CoinDesk publicó que Alameda Research, el fondo de trading de Sam Bankman-Fried, fundador de FTX, tenía una parte sustancial de su balance en FTT, el token propio del exchange (*Faux, 2023*). Las retiradas que siguieron a esa publicación revelaron que FTX no podía hacer frente a ellas: los fondos de los clientes habían sido utilizados por Alameda para sus propias operaciones. Bankman-Fried fue condenado por fraude y conspiración en noviembre de 2023.

Lo que hace a FTX difícil de ignorar, más allá de la magnitud del fraude, es el contexto en que ocurrió. Bankman-Fried era una figura activa en debates regulatorios en Washington, financiaba causas políticas y había construido públicamente una imagen de exchange responsable. Que todo eso coexistiera con una gestión fraudulenta de fondos de clientes sin que nadie lo detectara dice algo sobre los límites del due diligence en un mercado sin requisitos de auditoría ni segregación de activos obligatoria para los exchanges. BlockFi quebró semanas después. Genesis Global Capital suspendió retiradas en noviembre y se declaró en quiebra en enero de 2023. El contagio fue rápido.

3.4 La reacción de los organismos internacionales

La respuesta internacional al crecimiento del mercado cripto no fue un gran golpe sobre la mesa. Fue incremental: análisis, luego recomendaciones, luego marcos concretos. Sin el equivalente al Basilea III que siguió a 2008, al menos por ahora.

El Financial Stability Board ha liderado la coordinación. Su informe de 2022 identificó tres canales principales de riesgo sistémico: la exposición directa de instituciones reguladas, el uso de criptoactivos en sistemas de pagos, y los riesgos de confianza que pueden propagarse más allá del ecosistema cripto en episodios de fraude o colapso (*FSB, 2022*). En 2023 publicó recomendaciones basadas en el principio de que actividades equivalentes deben recibir tratamiento regulatorio equivalente, independientemente de la tecnología (*FSB, 2023*). Es un principio razonable, aunque su implementación práctica es más complicada de lo que sugiere la formulación.

El FMI ha contribuido principalmente con análisis sobre correlación entre mercados y sobre los riesgos macro-financieros de adoptar criptoactivos como moneda de curso legal, debate que cobró protagonismo cuando El Salvador adoptó bitcoin como moneda oficial en 2021 (*IMF,*

2022). La posición del Fondo ha sido consistentemente escéptica: la volatilidad hace a los criptoactivos inadecuados para las funciones básicas del dinero, y los riesgos para la estabilidad financiera de una economía dolarizada son considerables.

El Comité de Basilea publicó en 2022 su estándar para el tratamiento prudencial de las exposiciones bancarias a criptoactivos (*BCBS, 2022*). La distinción central es entre activos tokenizados asimilables a instrumentos tradicionales y criptoactivos sin respaldo como bitcoin, que reciben una ponderación por riesgo del 1.250%. En términos prácticos eso equivale a una deducción de capital: un banco que quiera tener exposición a bitcoin tiene que apartar capital propio equivalente al valor de esa posición. Es una forma de hacer la actividad regulatoriamente cara sin prohibirla directamente.

El problema de fondo de toda esta coordinación es geográfico. Los mercados cripto no tienen fronteras y los usuarios pueden acceder a exchanges o protocolos en cualquier jurisdicción. Mientras haya diferencias regulatorias entre países, habrá arbitraje. FTX, registrado en las Bahamas pero con operaciones globales y millones de usuarios en jurisdicciones reguladas, es el ejemplo más claro de cómo esa fragmentación genera vacíos con consecuencias concretas.

Capítulo 4: La respuesta regulatoria

4.1 El enfoque internacional: FSB, FMI y BIS

El marco regulatorio internacional que ha ido tomando forma en los últimos años no nació de un diseño previo sino de la acumulación de episodios que fueron dejando claro que el mercado cripto tenía consecuencias sobre el sistema financiero convencional. El Capítulo 3 analizó los canales de riesgo y la respuesta específica de cada organismo. Lo que interesa aquí es el principio que subyace a esa respuesta y sus limitaciones como marco de coordinación global.

El FSB, el FMI y el BIS han convergido en un diagnóstico común: los criptoactivos no son un fenómeno aislado y su regulación no puede dejarse exclusivamente en manos de las jurisdicciones individuales. La recomendación del FSB de 2023 de aplicar el principio de equivalencia regulatoria ("misma actividad, mismo riesgo, misma regulación") es el intento más articulado de trasladar ese diagnóstico a un principio operativo (*FSB, 2023*). La idea es sencilla: si un exchange de criptoactivos realiza funciones económicamente equivalentes a las de un broker tradicional, debería estar sujeto a requisitos similares de capital, conducta y transparencia, con independencia de la tecnología que use.

El problema es que ese principio es más fácil de enunciar que de implementar. Los mercados cripto tienen características que los diferencian estructuralmente de los mercados financieros tradicionales: operan de forma continua, no tienen horarios ni cierres, son accesibles desde cualquier jurisdicción y una parte relevante de su actividad ocurre en protocolos descentralizados sin un emisor o gestor identificable. Aplicar la regulación de un broker a un protocolo DeFi que no tiene accionistas, sede social ni empleados es un problema que ningún organismo internacional ha resuelto todavía.

La coordinación internacional tiene además un límite estructural: no es vinculante. Las recomendaciones del FSB o del BIS no obligan a ningún país a hacer nada. Su influencia opera a través de la presión entre pares y de la incorporación de sus estándares en los marcos regulatorios nacionales y regionales. Europa ha sido el ejemplo más avanzado de esa incorporación, con MiCA como resultado.

4.2 Europa: el Reglamento MiCA, DORA y el régimen DLT

El Reglamento de Mercados de Criptoactivos, conocido como MiCA, es el marco regulatorio más completo que existe hasta la fecha para el sector. Aprobado en 2023 y con plena aplicación desde finales de 2024, establece por primera vez un régimen armonizado para toda la Unión Europea que cubre tanto a los emisores de criptoactivos como a los proveedores de servicios sobre ellos, los llamados CASPs (Crypto-Asset Service Providers) (*Reglamento UE 2023/1114*).

El punto de partida de MiCA es una clasificación de los criptoactivos en tres categorías. Los tokens referenciados a activos (ARTs), que incluyen a las stablecoins respaldadas por una cesta de activos. Los tokens de dinero electrónico (EMTs), stablecoins referenciadas a una única moneda fiat. Y el resto de criptoactivos, que incluye a bitcoin, ether y la mayor parte de los tokens del mercado. Cada categoría tiene sus propios requisitos de emisión, reservas y conducta, siendo los más exigentes los que aplican a los ARTs y EMTs de mayor volumen, para los que se establecen límites de transacciones diarias y requisitos de reservas líquidas.

Para los CASPs, MiCA introduce un sistema de autorización similar al de los mercados financieros tradicionales. Cualquier empresa que quiera prestar servicios de custodia, intercambio, gestión de carteras o asesoramiento sobre criptoactivos en la UE necesita obtener una autorización de su supervisor nacional, que será reconocida en el resto de estados miembros mediante el pasaporte europeo. Los requisitos incluyen capital mínimo, segregación de activos de clientes, políticas de gestión de conflictos de interés y obligaciones de transparencia sobre precios y ejecución de órdenes.

MiCA también aborda la integridad del mercado. Prohíbe explícitamente el abuso de mercado en criptoactivos, incluyendo el uso de información privilegiada y la manipulación de precios, y atribuye competencias sancionadoras a los supervisores nacionales. Es un cambio relevante respecto a la situación anterior, en la que prácticas como el wash trading o el pump-and-dump operaban en un vacío legal en gran parte de las jurisdicciones europeas.

Lo que MiCA no cubre es igualmente importante. Los protocolos DeFi quedan fuera de su ámbito de aplicación cuando son suficientemente descentralizados, es decir, cuando no hay un intermediario identificable que preste el servicio. Los NFT también quedan fuera en la mayoría de los casos. Y bitcoin y ether, como criptoactivos sin emisor identificable, solo están sujetos a MiCA cuando son objeto de servicios prestados por CASPs autorizados, no en sus transacciones peer-to-peer. Esta delimitación es coherente con el enfoque de regular a los intermediarios más que a los protocolos, pero deja sin cubrir una parte significativa de la actividad del ecosistema.

Junto a MiCA, dos marcos complementarios completan el panorama regulatorio europeo para el sector. DORA, el Reglamento de Resiliencia Operativa Digital, establece requisitos de ciberseguridad y gestión del riesgo tecnológico para las entidades financieras, incluyendo a los CASPs autorizados bajo MiCA (*Reglamento UE 2022/2554*). Y el Reglamento del Régimen Piloto para las infraestructuras de mercado basadas en tecnología DLT permite a las entidades operar mercados secundarios de instrumentos financieros tokenizados bajo un régimen de excepciones temporales respecto a la regulación financiera tradicional, con el objetivo de generar experiencia regulatoria antes de modificar definitivamente los marcos existentes (*Reglamento UE 2022/858*).

En España, la transposición de MiCA se articula principalmente a través de la CNMV como supervisor competente para la autorización de CASPs, con el Banco de España asumiendo competencias en materia de emisores de tokens de dinero electrónico. El registro previo de proveedores de servicios de criptoactivos que el Banco de España venía manteniendo desde 2022 en cumplimiento de la normativa anti-blanqueo se integra en el nuevo marco de autorización de MiCA.

4.3 Estados Unidos y la fragmentación regulatoria

Si Europa ha optado por la claridad regulatoria a través de un marco armonizado, Estados Unidos representa el caso opuesto: un mercado enorme, con una industria cripto muy desarrollada, pero sin un marco federal coherente para regularla.

El problema de fondo es competencial. La SEC, la Comisión de Valores, y la CFTC, la Comisión de Comercio de Futuros, disputan la jurisdicción sobre distintos tipos de criptoactivos desde hace años. La SEC sostiene que la mayoría de los tokens son valores (securities) bajo el test de Howey y por tanto están sujetos a su supervisión. La CFTC considera

que bitcoin y ether son materias primas (commodities) y caen bajo su competencia. Para el resto del mercado, la línea entre ambas categorías es objeto de litigios activos, con la SEC habiendo iniciado procedimientos sancionadores contra exchanges como Coinbase y Binance por operar mercados de valores no registrados (*SEC v. Coinbase, 2023*).

Esta ambigüedad tiene consecuencias prácticas para las empresas del sector. Operar en Estados Unidos implica navegar una incertidumbre regulatoria que hace difícil planificar el negocio a largo plazo. Varios emisores de tokens han optado por estructuras legales que les permiten argumentar que sus activos no son valores, con resultados judiciales mixtos. Y los exchanges han tenido que tomar decisiones sobre qué activos listar basándose en análisis jurídicos propios ante la ausencia de criterios regulatorios claros.

El Congreso ha intentado en varias ocasiones aprobar legislación que resuelva este conflicto de jurisdicción, sin éxito hasta la fecha. Las propuestas más avanzadas han buscado atribuir a la CFTC la supervisión de los criptoactivos que funcionan como materias primas digitales, reservando a la SEC los que tienen características de valores. Pero las diferencias políticas sobre el alcance de la regulación y la resistencia de ambas agencias a ceder competencias han impedido un acuerdo legislativo.

El resultado es que el mercado cripto estadounidense opera en un entorno donde las reglas se establecen principalmente a través de la litigación y de las acciones de enforcement de las agencias reguladoras, más que a través de legislación clara. Eso genera costes para las empresas que quieren operar dentro de la ley, y oportunidades para las que prefieren operar en la frontera de la misma.

4.4 Efectos sobre los inversores y el mercado

La respuesta regulatoria tiene efectos sobre la estructura del mercado y sobre el comportamiento de los inversores que van más allá del cumplimiento normativo.

El efecto más inmediato es la concentración. Los requisitos de capital, autorización y cumplimiento que impone MiCA, y que los marcos regulatorios de otras jurisdicciones replicarán en mayor o menor medida, favorecen a los actores con más recursos para absorber esos costes. Un exchange pequeño o una startup de servicios cripto puede encontrar que el coste de obtener y mantener una autorización bajo MiCA es prohibitivo. El resultado previsible es una consolidación del mercado en torno a un número menor de operadores grandes, lo que reproduce en el sector cripto la dinámica de concentración que caracteriza a los mercados financieros tradicionales (*FSB, 2023*).

Para los inversores minoristas, la regulación tiene un efecto doble. Por un lado, ofrece protecciones que antes no existían: segregación de activos, transparencia sobre precios, prohibición de prácticas manipuladoras y, en algunos casos, acceso a mecanismos de reclamación. Por otro, el endurecimiento de los requisitos KYC y AML reduce la posibilidad de acceder al mercado de forma anónima, lo que choca con uno de los principios originales del proyecto cripto.

La aprobación de los ETF de bitcoin al contado en Estados Unidos en 2024 ilustra bien esta tensión. Para un inversor institucional o para alguien que prefiere no gestionar sus propias claves privadas, los ETF son un avance: ofrecen exposición a bitcoin con la comodidad y las protecciones de un producto financiero regulado. Para alguien que valora la autocustodia y la

resistencia a la censura como propiedades fundamentales de bitcoin, los ETF son irrelevantes o incluso contraproducentes, porque concentran la propiedad efectiva del activo en custodios institucionales y refuerzan el papel de los intermediarios financieros que bitcoin pretendía hacer innecesarios.

Esta divergencia entre tipos de inversores refleja una fragmentación más profunda del mercado cripto. Ya no hay un único perfil de participante. Conviven inversores institucionales que buscan exposición a un activo de alta volatilidad dentro de un marco regulado, usuarios que utilizan protocolos DeFi para acceder a servicios financieros sin intermediarios, y personas en países con monedas inestables que usan stablecoins como sustituto del dólar. La regulación que sirve bien a los primeros no necesariamente sirve a los segundos o a los terceros, lo que hace que el diseño de un marco regulatorio globalmente adecuado sea un problema sin solución evidente.

Capítulo 5: ¿Siguen siendo un proyecto de libertad económica?

5.1 La paradoja de la descentralización: concentración de poder en un sistema que prometía eliminarlo

Bitcoin nació con una promesa concreta: un sistema en el que ningún actor individual pudiera controlar el flujo de valor de otro. Sin bancos, sin intermediarios, sin posibilidad de censura. Esa promesa tenía una base técnica real en 2009. La pregunta que se impone después de los capítulos anteriores es si esa base técnica sigue siendo suficiente para sostener la promesa, o si la evolución del ecosistema la ha vaciado de contenido.

La respuesta honesta es que depende de dónde se mire. El protocolo de Bitcoin no ha cambiado de forma sustancial. La emisión sigue el mismo calendario fijo, el consenso funciona igual, el registro sigue siendo inmutable. Nada de eso ha variado. Lo que sí ha cambiado es todo lo que rodea al protocolo, y ahí es donde aparecen las nuevas formas de concentración.

La minería es el primer ejemplo. En teoría, cualquier persona con un ordenador puede participar en la validación de la red. En la práctica, la competencia por el hashrate ha llevado a una concentración progresiva en grandes pools de minería. Los cinco mayores pools controlan consistentemente más del 50% del poder de cómputo de la red Bitcoin (*Blockchain.com, 2024*). Eso no significa que la red esté controlada por cinco actores, porque los mineros individuales pueden cambiar de pool. Pero sí significa que si esos pools coordinaran sus acciones, tendrían la capacidad técnica de ejecutar un ataque del 51%. La descentralización del hashrate es real en teoría y frágil en la práctica.

Los exchanges centralizados son el segundo ejemplo, y el más relevante para el usuario medio. La narrativa original de Bitcoin es la de la autocustodia: tus claves, tu dinero. Coinbase, Binance y Kraken custodian los activos de la mayoría de sus usuarios. Cuando FTX colapsó, nadie perdió acceso a sus bitcoins porque el protocolo fallara. Lo perdieron porque habían cedido la custodia a un intermediario que resultó ser fraudulento. La promesa de resistencia a la censura no sirve de nada si el usuario no controla sus propias claves. Y la mayoría no las controla, porque hacerlo tiene una complejidad operativa que pocos están dispuestos a asumir. El resultado práctico es que los grandes exchanges son gatekeepers de facto: pueden congelar cuentas, rechazar transacciones y, bajo marcos regulatorios como MiCA, están obligados a hacerlo en ciertas circunstancias (*FSB, 2023*).

La concentración de la propiedad añade otra capa. Foley et al. (2019) estimaron que el 1% de las direcciones controlaba más del 27% del supply en circulación. Cuando esas posiciones se mueven, el mercado lo siente. La concentración de riqueza existe en todos los mercados, pero resulta llamativa en uno que se presentó como alternativa igualitaria al sistema financiero tradicional.

El desarrollo del protocolo sigue una lógica parecida. En teoría, cualquier cambio en Bitcoin requiere consenso amplio de la comunidad. En la práctica, Bitcoin Core concentra la influencia técnica de facto. Los desarrolladores de ese cliente no tienen mandato formal ni mecanismo de elección, pero sus decisiones determinan la dirección del protocolo. Es descentralización con asterisco.

En Ethereum el problema se ha desplazado desde la minería hacia el staking. Lido concentra más del 30% del ETH en staking (*DefiLlama, 2024*), y los tokens de gobernanza de los

principales protocolos DeFi reproducen las estructuras del capital riesgo tradicional. La gobernanza descentralizada sigue siendo más aspiración que realidad.

Lo que todo esto apunta no es que Bitcoin o Ethereum hayan fallado como tecnologías. El protocolo puede funcionar perfectamente y estar rodeado de infraestructura completamente centralizada. Para la mayoría de los usuarios, lo que importa es la infraestructura (*Böhme et al., 2015*).

5.2 La transformación de la demanda: del usuario ideológico al inversor institucional

El cambio en quién participa en el mercado cripto es tan relevante para responder la pregunta central como el cambio en la estructura del ecosistema. Los dos están conectados: la demanda moldea la oferta, y la oferta cambia quién puede participar.

En sus primeros años el mercado tenía un perfil muy específico. Programadores atraídos por la tecnología, libertarios que veían en Bitcoin una herramienta de resistencia frente al control estatal, activistas que financiaban causas que los sistemas convencionales rechazaban, y especuladores tempranos con tolerancia alta al riesgo. Con distintos matices, todos compartían una orientación hacia la desintermediación y la soberanía individual.

Ese perfil ha cambiado de forma sustancial. La entrada de capital institucional descrita en el Capítulo 2 no es solo un cambio en el tamaño del mercado; es un cambio en los objetivos de sus participantes dominantes. Un fondo de pensiones que compra un ETF de bitcoin no busca resistencia a la censura ni soberanía monetaria. Busca diversificación de cartera y exposición a un activo de alta volatilidad con potencial de revalorización. MicroStrategy no convirtió su tesorería en bitcoin porque desconfíe del sistema bancario; lo hizo como estrategia de gestión de balance. BlackRock no lanzó un ETF de bitcoin porque crea en la descentralización; lo hizo porque había demanda de sus clientes institucionales.

Esta transformación de la demanda tiene consecuencias sobre el propio activo. El precio de bitcoin, que en sus primeros años respondía principalmente a dinámicas internas del ecosistema, está cada vez más correlacionado con los ciclos de apetito por el riesgo de los mercados financieros globales (*IMF, 2022*). Cuando la Reserva Federal sube los tipos de interés, bitcoin cae junto con las acciones de crecimiento. Cuando los mercados recuperan el optimismo, bitcoin sube. Esa correlación no existía hace diez años. Es la consecuencia directa de que el capital que mueve el precio sea en buena medida el mismo capital que mueve el resto de los mercados financieros.

La adopción corporativa tiene un efecto paradójico. MicroStrategy compra bitcoin y el precio sube. En mayo de 2021, Elon Musk anunció que Tesla dejaba de aceptar bitcoin como medio de pago y el precio cayó un 15% en horas. Un activo cuyo precio se mueve así con los tweets de un CEO o los comunicados de una empresa cotizada no encaja bien con la imagen del dinero soberano e independiente que describía el whitepaper de Nakamoto.

La fragmentación del mercado que describe el final del Capítulo 4 refleja esta tensión. Conviven en el mismo ecosistema inversores institucionales que usan bitcoin como activo de reserva, usuarios de DeFi que buscan servicios financieros sin intermediarios, y personas en países con monedas inestables que usan stablecoins como sustituto del dólar. Estos tres grupos

tienen objetivos tan distintos que la pregunta de si las criptomonedas siguen siendo un proyecto de libertad económica no tiene una respuesta única. Depende de para quién.

5.3 Innovación, regulación y poder de mercado: ¿puede existir libertad económica real en un mercado institucionalizado?

La pregunta que da título a este capítulo no admite una respuesta binaria. Las criptomonedas no son ni el sistema de libertad económica absoluta que prometían sus fundadores ni un activo financiero convencional más. Son las dos cosas a la vez, en proporciones distintas según el ángulo. El protocolo de Bitcoin no ha cambiado desde 2009. Quien controla sus propias claves puede enviar valor a cualquier persona del mundo sin pedir permiso, sin que un banco lo bloquee y sin que un gobierno lo confisque fácilmente. Eso sigue siendo cierto. Y sigue siendo relevante: el uso de bitcoin y stablecoins en Venezuela, Argentina o Turquía no es retórica ideológica, es una respuesta a fallos concretos del sistema financiero local.

Pero esa propiedad técnica coexiste con un ecosistema que ha evolucionado en una dirección opuesta al ideal original. La regulación ha introducido intermediarios obligatorios en los puntos de entrada y salida del ecosistema. La institucionalización ha concentrado el capital y la influencia en actores que no comparten los objetivos de los fundadores del movimiento. Y la complejidad creciente del ecosistema ha alejado al usuario medio de la autocustodia y la participación directa, empujándolo hacia plataformas centralizadas que reproducen la lógica de los intermediarios financieros que Bitcoin pretendía hacer innecesarios.

¿Es eso un fracaso? Depende del criterio. Si el criterio es la adopción masiva y el reconocimiento como clase de activo, el ecosistema cripto ha tenido un éxito notable. Si el criterio es la realización del ideal original de desintermediación y soberanía individual, el balance es más ambiguo. La integración en el sistema financiero convencional ha traído legitimidad y liquidez, pero también ha importado las mismas dinámicas de concentración, intermediación y captura regulatoria que el proyecto pretendía evitar.

Hay un argumento que los defensores del ecosistema esgrimen con frecuencia: que la infraestructura centralizada que rodea a los protocolos descentralizados es una capa separable, y que la descentralización del protocolo garantiza que siempre existirá una alternativa al uso de intermediarios para quien esté dispuesto a asumirlo. El argumento tiene mérito técnico. Pero en la práctica, la alternativa descentralizada requiere un nivel de competencia técnica y tolerancia al riesgo operativo que la excluye para la mayoría de los usuarios. La libertad económica que depende de saber gestionar claves criptográficas no es libertad económica para el ciudadano medio; es libertad económica para una minoría técnicamente competente.

La tensión entre la promesa original y la realidad actual no es únicamente el resultado de decisiones equivocadas o de la traición a unos principios. Es en buena medida el resultado lógico del crecimiento. Un ecosistema que permanece pequeño y marginal puede mantener sus principios de pureza ideológica con más facilidad que uno que aspira a ser relevante a escala global. La pregunta de si es posible construir un sistema financiero alternativo que sea simultáneamente accesible, seguro, regulado y descentralizado no tiene respuesta evidente. Lo que la evolución del ecosistema cripto ha demostrado, al menos hasta ahora, es que escalar esos cuatro atributos a la vez es enormemente difícil.

Conclusiones

Este trabajo partía de una pregunta: si las criptomonedas siguen siendo el proyecto de libertad económica que les dio origen o si se han convertido en un activo financiero más dentro del sistema regulado. La respuesta que emerge del análisis es incómoda en su ambigüedad: las dos cosas son ciertas a la vez, y la tensión entre ellas es lo que mejor define el estado actual del ecosistema.

Síntesis de los hallazgos

El recorrido por los cinco capítulos deja varias ideas asentadas. Para empezar, el proyecto original de Bitcoin respondía a una motivación concreta y legítima. La desconfianza en un sistema financiero que la crisis de 2008 había dejado en evidencia no era paranoia ideológica, y los principios de desintermediación, control individual y reglas monetarias transparentes eran una propuesta de solución a problemas reales.

Esa propuesta evolucionó. El paso de Bitcoin hacia Ethereum y las finanzas descentralizadas amplió enormemente lo que el ecosistema podía hacer, pero a cambio lo volvió mucho más complejo. Minar para conseguir monedas era algo que cualquiera podía entender. El modelo actual, con su staking, su provisión de liquidez y su gobernanza tokenizada, exige una sofisticación que deja fuera a buena parte de los usuarios. La accesibilidad de los primeros años se perdió por el camino.

Esa misma evolución trajo riesgos financieros de peso. La interconexión creciente con el sistema tradicional, la volatilidad estructural, la concentración de la propiedad y la velocidad del contagio quedaron al descubierto en los colapsos de 2022. Terra-Luna y FTX no fueron accidentes aislados, sino síntomas de un mercado que había crecido más rápido que sus propios mecanismos de control. Y fueron, en buena medida, los que aceleraron la respuesta regulatoria.

Esa regulación es el último eslabón de la transformación. Aporta protecciones reales a los inversores, pero introduce intermediarios obligatorios y favorece la concentración del mercado en torno a quienes pueden permitirse los costes de cumplimiento. En sus puntos de entrada y salida, el ecosistema cripto se parece cada vez más al sistema financiero que Bitcoin quería dejar atrás.

Evaluación de la hipótesis

La hipótesis del inicio se confirma en lo esencial. La transformación de las criptomonedas, de proyecto de libertad económica a activo financiero institucionalizado, ha sido real y profunda. La concentración en pools de minería, el dominio de los exchanges centralizados como puerta de entrada, la llegada de los custodios institucionales y la concentración del voto en los protocolos DeFi reproducen, con otros nombres, las dinámicas del sistema que se quería superar.

Pero la hipótesis también anticipaba que la transformación no sería total, y eso se cumple igualmente. El protocolo de Bitcoin sigue intacto en lo técnico. Quien controla sus claves puede transferir valor sin permiso y sin intermediarios, y en lugares con represión financiera o monedas que se desploman, esa posibilidad no es un detalle teórico sino una herramienta que la gente usa.

La conclusión más matizada, y quizá la más relevante, es que la respuesta depende de quién pregunte. Para el fondo que compra un ETF, las criptomonedas son un activo financiero más. Para quien vive en un país con hiperinflación y recurre a stablecoins, son una vía de supervivencia. Para el partidario de la autocustodia, siguen siendo soberanía individual. Las tres cosas son verdad a la vez, en el mismo ecosistema.

Reflexiones finales

El caso de las criptomonedas ilustra una tensión más amplia sobre el destino de las innovaciones financieras. Un sistema que aspira a ser relevante a escala global difícilmente puede conservar intactos sus principios fundacionales. El crecimiento arrastra institucionalización, regulación y concentración casi por inercia. Lo que este caso demuestra es que escalar a la vez accesibilidad, seguridad, cumplimiento normativo y descentralización es enormemente difícil, y que avanzar en unos de esos frentes suele costar terreno en otros.

Queda abierta la pregunta de si cabía un equilibrio distinto. Los defensores del ecosistema insisten en que la capa descentralizada del protocolo garantiza que siempre habrá una alternativa para quien la quiera. El análisis de este trabajo sugiere que esa alternativa, aunque técnicamente exista, solo es practicable para una minoría con la competencia técnica suficiente. La libertad económica que prometía Bitcoin no ha desaparecido, pero se ha vuelto minoritaria dentro de un mercado que, en su mayor parte, ha elegido integrarse. Si eso es el fracaso del proyecto original o simplemente la forma que toma su madurez es, al final, una cuestión de perspectiva.

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado

Por la presente, yo, Santiago Núñez Clavijo, estudiante de ADE con mención internacional (E-4) de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "DE LA DESCENTRALIZACIÓN A LA REGULACIÓN: ¿SIGUEN SIENDO LAS CRIPTOMONEDAS UN PROYECTO DE LIBERTAD ECONÓMICA?", declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. Brainstorming de ideas de investigación: Utilizado para idear y esbozar posibles áreas de investigación.
2. Crítico: Para encontrar contra-argumentos a una tesis específica que pretendo defender.
3. Corrector de estilo literario y de lenguaje: Para mejorar la calidad lingüística y estilística del texto.
4. Traductor: Para traducir textos de un lenguaje a otro.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 02/06/2026



Firma:

Bibliografía

- Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). Uniswap v3 Core. Uniswap Labs.
- Acharya, V. V., Richardson, M., van Nieuwerburgh, S., & White, L. J. (2009). Guaranteed to Fail.
- BCBS (2022). Prudential treatment of cryptoasset exposures. Basel Committee on Banking Supervision.
- Biais, B., Bisière, C., Bouvard, M., Casamatta, C., & Menkveld, A. J. (2023). Equilibrium Bitcoin Pricing. *Journal of Finance*, 78(2), 967-1014.
- BIS (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*.
- BIS (2022). Stablecoins: risks, regulation and central bank oversight. *BIS Papers No 123*.
- Blockchain.com (2024). Hashrate Distribution by Mining Pool. Consultado en <https://www.blockchain.com/explorer/charts/pools>
- Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2023). Anatomy of a Stablecoin's failure: The Terra-Luna case. *Finance Research Letters*, 51, 103358.
- Brunnermeier, M. K. (2009). Deciphering the Liquidity and Credit Crunch 2007-2008. *Journal of Economic Perspectives*.
- Budish, E. (2018). The Economic Limits of Bitcoin and the Blockchain. NBER Working Paper No. 24717.
- Buterin, V. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*.
- Cornelli, G., Doerr, S., Frost, J., & Gambacorta, L. (2023). Crypto shocks and retail losses. *BIS Bulletins*, No. 69. Bank for International Settlements.
- DefiLlama (2024). Liquid Staking TVL Dashboard. Consultado en <https://defillama.com/protocols/liquid%20staking>
- Faux, Z. (2023). Number Go Up: Inside Crypto's Wild Rise and Staggering Fall. *Currency*.
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *Review of Financial Studies*.
- FSB (2022). Assessment of Risks to Financial Stability from Crypto-assets. *Financial Stability Board*.
- FSB (2023). FSB Global Regulatory Framework for Crypto-asset Activities. *Financial Stability Board*.
- FSB (2024). Global Monitoring Report on Crypto-Assets. *Financial Stability Board*.
- Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2021). Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics*.
- Gorton, G. (2010). Slapped by the Invisible Hand.
- Heimbach, L., Kiffer, L., Ferreira, C., & Wattenhofer, R. (2023). Ethereum's Proof of Stake Consensus Mechanism and its Effect on Liquid Staking. *Working Paper*.
- IMF (2022). Global Financial Stability Report: Shockwaves from the War in Ukraine Test the Financial System's Resilience. *International Monetary Fund*.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

- Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro distribuido.
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA).
- Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA).
- Reinhart, C. M., & Rogoff, K. (2009). This Time is Different.
- SEC v. Coinbase, Inc. (S.D.N.Y., filed June 6, 2023). Complaint available at: <https://www.sec.gov/enforcement-litigation/litigation-releases/lr-25751>
- Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper.