UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DSIC
DEPARTAMENT DE SISTEMES INFORMÀTICS I COMPUTACIÓ

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Dpto. de Sistemas Informáticos y Computación

Revisión y estudio de técnicas de escalado en sistemas blockchain

Trabajo Fin de Máster

Máster Universitario en Computación en la Nube y de Altas Prestaciones / Cloud and High-Performance Computing

AUTOR/A: Tomás Sanjuan, Rafael

Tutor/a: Muñoz Escoí, Francisco Daniel

CURSO ACADÉMICO: 2024/2025

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DSIC DEPARTAMENTO DE SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

Dpto. de Sistemas Informáticos y Computación

Trabajo fin de máster

Revisión y estudio de técnicas de escalado en sistemas blockchain

Máster Universitario en Computación en la Nube y de Altas Prestaciones / Cloud and High-Performance Computing

Autor:

Tomás Sanjuan, Rafael

Tutor/a:

Muñoz Escoí, Francisco Daniel

Curso académico: 2024-2025 Convocatoria: Septiembre 2025

Resumen

Los sistemas blockchain surgieron en 2008 como la tecnología subyacente de Bitcoin. Esta propuesta inicial se fundamentó en tres pilares: descentralización, inmutabilidad de los registros y anonimato de los participantes. Para que un nuevo bloque sea aceptado en la cadena, los nodos de la red deben alcanzar un consenso, un proceso de coordinación que inherentemente limita la escalabilidad del sistema. Como respuesta, emergieron las redes blockchain permisionadas, donde el acceso restringido a un conjunto de participantes conocidos permite el uso de algoritmos de consenso más eficientes. Sin embargo, para los sistemas públicos, donde la participación es abierta, se han desarrollado otras soluciones para mejorar la escalabilidad, tales como canales de pago, sidechains, sharding y protocolos de Capa 2 (L2). Este Trabajo de Fin de Máster (TFM) presenta una revisión de la evolución histórica de estas propuestas, analizando los mecanismos que emplean para optimizar el rendimiento de los sistemas blockchain.

Resum

Els sistemes blockchain van sorgir en 2008 com la tecnologia subjacent de Bitcoin. Aquesta proposta inicial es va fonamentar en tres pilars: descentralització, immutabilitat dels registres i anonimat dels participants. Perquè un nou bloc siga acceptat en la cadena, els nodes de la xarxa han d'arribar a un consens, un procés de coordinació que inherentment limita l'escalabilitat del sistema. Com a resposta, van emergir les xarxes blockchain permissionades, on l'accés restringit a un conjunt de participants coneguts permet l'ús d'algorismes de consens més eficients. No obstant això, per als sistemes públics, on la participació és oberta, s'han desenvolupat altres solucions per a millorar l'escalabilitat, tals com canals de pagament, sidechains, sharding i protocols de L2. Aquest TFM presenta una revisió de l'evolució històrica d'aquestes propostes, analitzant els mecanismes que empren per a optimitzar el rendiment dels sistemes blockchain.

Abstract

Blockchain systems emerged in 2008 as the underlying technology of Bitcoin. This initial proposal was founded on three pillars: decentralization, immutability of records, and anonymity of participants. For a new block to be accepted into the chain, network nodes must reach a consensus, a coordination process that inherently limits system scalability. In response, permissioned blockchain networks emerged, where restricted access to a set of known participants allows the use of more efficient consensus algorithms. However, for public systems, where participation is open, other solutions have been developed to improve scalability, such as payment channels, sidechains, sharding, and L2 protocols. This TFM presents a review of the historical evolution of these proposals, analyzing the mechanisms they employ to optimize the performance of blockchain systems.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción

1.1. El nacimiento de Bitcoin y la tecnología blockchain

La era digital ha transformado radicalmente el intercambio de información, pero ha enfrentado un desafío fundamental: replicar la confianza en un entorno nativo digital. En el mundo físico, la confianza se delega en instituciones centrales como bancos, gobiernos y notarios, que actúan como intermediarios para validar transacciones. Sin embargo, la réplica de este modelo centralizado en internet hereda y amplifica sus vulnerabilidades intrínsecas: la censura, los costes operativos y la existencia de puntos únicos de fallo.

Frente a este paradigma, surgió una pregunta fundamental: ¿Es posible crear un sistema de intercambio de valor Entre Pares (P2P) que no dependa de un tercero de confianza? La aspiración de concebir un dinero puramente digital, privado y resistente al control se enfrentaba a un obstáculo técnico crítico: el "problema del doble gasto". Este consiste en impedir que una misma unidad de dinero digital se utilice más de una vez en un entorno descentralizado, donde ninguna autoridad central supervisa las transacciones.

La solución llegó en 2008 con la publicación del libro blanco de Bitcoin por una figura anónima bajo el seudónimo de Satoshi Nakamoto, que presentaba un "sistema de efectivo electrónico entre pares" (Nakamoto, 2008). Este hito no fue un evento aislado, sino la culminación de décadas de avances previos en criptografía y sistemas distribuidos.

La gestación de Bitcoin se nutrió de pilares criptográficos clave. En la década de 1980, David Chaum concibió *eCash*, un sistema pionero en privacidad que empleaba *firmas ciegas* para permitir que un banco firmara digitalmente una moneda sin

conocer su contenido, garantizando así el anonimato del pagador (Chaum, 1983). No obstante, su diseño centralizado constituía una debilidad insalvable para el objetivo de la resistencia a la censura. A la privacidad se sumó la búsqueda de la inmutabilidad, lograda conceptualmente en 1991 por Stuart Haber y W. Scott Stornetta. Su método de encadenamiento secuencial de documentos mediante *hashes* criptográficos (donde cada nuevo registro incluye el hash del anterior) es el precursor técnico directo de una "blockchain" (Haber & Stornetta, 1991). El último pilar fue la Prueba de Trabajo (PoW), cuya implementación más influyente, *Hashcash* de Adam Back (Back, 2002), fue ingeniosamente adaptada por Nakamoto para constituir el núcleo de su algoritmo de consenso, un mecanismo que no solo aseguraba la red, sino que también regulaba la creación de nueva moneda.

Paralelamente, ya existían diseños conceptuales como "b-money" de Wei Dai (Dai, 1998) y "bit gold" de Nick Szabo (Szabo, 2005). Ambos eran sistemas visionarios de dinero distribuido que, sin embargo, no llegaron a materializarse. Su principal escollo fue la incapacidad de ofrecer una solución robusta al problema de los generales bizantinos, un famoso dilema de la computación distribuida que plantea cómo múltiples agentes pueden consensuar una única verdad si algunos de ellos pueden ser maliciosos o fallar. Sin una solución a este problema, la red no podía garantizar de forma fiable el estado correcto del libro contable, dejando la puerta abierta al doble gasto.

El mérito de Satoshi Nakamoto no residió, por tanto, en la invención de una tecnología *ex novo*, sino en la síntesis magistral de estas ideas preexistentes en un sistema funcional y robusto. Nakamoto utilizó la PoW no solo como barrera antispam, sino como la solución económica al problema de los generales bizantinos: al hacer que la creación de un bloque fuera computacionalmente costosa pero fácil de verificar, incentivó la cooperación honesta y penalizó los ataques, que requerirían un poder computacional prohibitivo. Al integrar esta solución con una estructura de cadena de hashes y una red de comunicación entre pares, nació Bitcoin y la tecnología que lo sustenta, la blockchain: la primera solución práctica al desafío de un sistema de dinero digital sin una entidad central de confianza (Rao et al., 2024).

1.2. El desafío de la adopción masiva

El diseño original de la blockchain, que priorizaba la seguridad y la descentralización, demostró ser una solución robusta y resistente a la censura. Sin embargo, estas mismas fortalezas revelaron una debilidad inherente al considerar su aplica-

ción a escala global: el rendimiento. Bitcoin puede procesar un máximo teórico de 7 Transacción por Segundo (TPS), mientras que Ethereum, en su configuración de PoW, gestiona entre 15 y 20 TPS (Zhou et al., 2020). Estas cifras son insuficientes para competir con sistemas de pago tradicionales; la red Visa, por ejemplo, procesa una media de 24,000 TPS y está diseñada para soportar picos superiores a 65,000 TPS (Visa Inc., 2023). Esta vasta diferencia de rendimiento, conocida como el "problema de la escalabilidad", constituye el principal obstáculo para la adopción masiva de las blockchains públicas (Rebello et al., 2024).

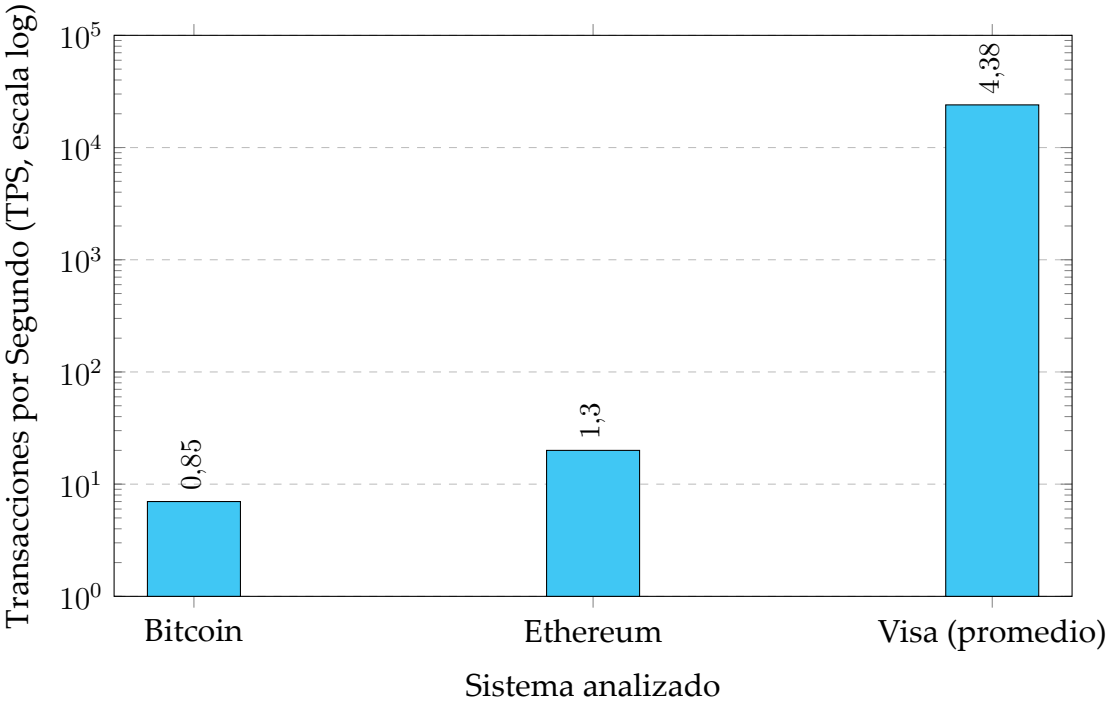

Figura 1.1: Comparativa de rendimiento entre blockchains públicas y sistemas de pago tradicionales. La escala logarítmica del eje Y evidencia la diferencia de órdenes de magnitud en la capacidad de procesamiento (TPS) entre Bitcoin o Ethereum y la red Visa (Visa Inc., 2023; Zhou et al., 2020).

El origen de esta limitación reside en la propia arquitectura de la red. A diferencia de un sistema centralizado, en una blockchain pública cada nodo completo debe, por diseño, procesar, validar y almacenar cada transacción. Este mecanismo de replicación redundante, esencial para la seguridad y la resiliencia, crea un cuello de botella computacional y de ancho de banda a escala de red (Nasir et al., 2022). Además, los parámetros del protocolo, como el tamaño máximo del bloque (aprox. 1 MB en Bitcoin) y el intervalo de generación (aprox. 10 minutos), se establecieron de forma conservadora para garantizar un consenso global y permitir la participación de nodos con recursos modestos, evitando así la centralización. No obstante, estos límites imponen una restricción física al volumen de transacciones que la

red puede procesar por unidad de tiempo (Hafid et al., 2020).

Este conflicto se articula en el trilema de la blockchain, popularizado por Vitalik Buterin (Buterin, 2017). El trilema postula que es un desafío fundamental optimizar simultáneamente tres propiedades deseables: *seguridad*, *descentralización* y *escalabilidad*. La tesis es que cualquier mejora significativa en una de estas propiedades tiende a degradar al menos una de las otras dos. Por ejemplo, aumentar drásticamente el tamaño del bloque para mejorar la *escalabilidad* (más TPS) incrementaría los requisitos de hardware y ancho de banda, lo que probablemente conduciría a una mayor *centralización*, ya que menos participantes podrían permitirse ejecutar un nodo completo. En esencia, todas las soluciones de escalado que se exploran en este trabajo representan diferentes estrategias para navegar este trilema.

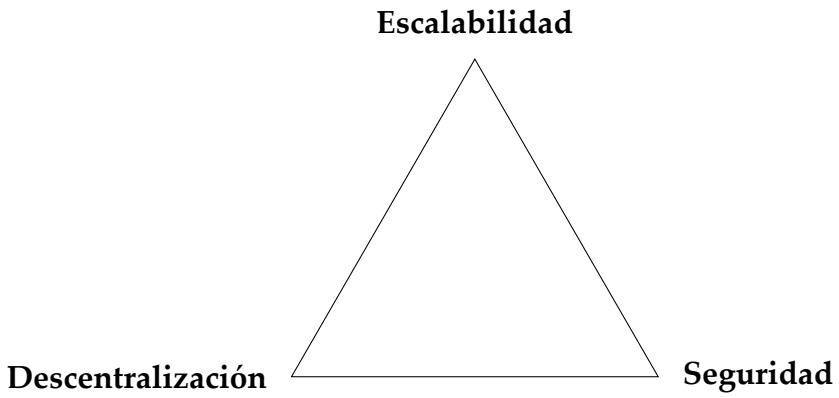

Figura 1.2: Representación visual del Trilema de la Blockchain como la formalización de la tensión entre escalabilidad y el coste de la verificación descentralizada.

Las consecuencias prácticas de esta limitación de rendimiento son directas y severas. En periodos de alta demanda, la red se congestiona y el espacio en los bloques se convierte en un recurso escaso, dando lugar a un "mercado de comisiones" donde los usuarios compiten con tarifas más altas para que sus transacciones sean priorizadas. Esto ha provocado que simples transacciones hayan llegado a costar decenas o cientos de dólares, haciendo inviable el uso de la red para micropagos. Adicionalmente, la congestión genera tiempos de confirmación largos e impredecibles. Esta combinación de altas comisiones y latencia es lo que ha impulsado la intensa actividad de investigación y desarrollo en torno a las soluciones de escalado, el tema central de este trabajo.

1.3. Justificación y relevancia del estudio

La resolución del problema de la escalabilidad no es un mero desafío técnico, sino la clave para desbloquear el potencial transformador de la tecnología blockchain. Sus aplicaciones se extienden más allá de las criptomonedas y podrían redefinir la interacción entre ciudadanos, gobiernos e instituciones financieras, reforzando la libertad individual, la eficiencia y la transparencia. La superación de estas barreras de rendimiento es, por tanto, un paso indispensable para que la blockchain transite del nicho tecnológico a la infraestructura global.

Como señalan diversas revisiones sistemáticas, la tecnología blockchain ya se explora en una amplia gama de sectores, como la sanidad, la Inteligencia Artificial (IA), el sector gubernamental y el Internet de las Cosas (IoT) (Hafid et al., 2020). En el ámbito sanitario, una blockchain escalable podría soportar sistemas de historiales médicos electrónicos interoperables y seguros, garantizando la privacidad del paciente y facilitando la investigación médica (Nasir et al., 2022). En el IoT, donde miles de millones de dispositivos necesitan interactuar y realizar micropagos de forma segura, la escalabilidad es un requisito no negociable para permitir una verdadera economía máquina a máquina (Sanka & Cheung, 2021).

Para gobiernos y entidades financieras, la capacidad de procesar un alto volumen de transacciones es fundamental para aplicaciones como la gestión de registros de propiedad, sistemas de votación o la modernización de los pagos transfronterizos. Sin embargo, como apuntan Hafid et al. (Hafid et al., 2020), estas aplicaciones a menudo requieren un rendimiento de miles de transacciones por segundo, una cifra que las blockchains actuales no pueden alcanzar.

Por tanto, comprender y categorizar las soluciones a este problema es crucial. Este estudio se justifica por la necesidad de ofrecer una visión estructurada y actualizada de un panorama tecnológico en vertiginosa evolución. Un análisis exhaustivo como el que se propone sirve como guía para desarrolladores, que deben elegir la arquitectura correcta; para investigadores, que buscan identificar desafíos no resueltos; y para inversores, que necesitan evaluar la viabilidad de los distintos proyectos. Sin una solución al problema de la escalabilidad, el impacto de la tecnología blockchain quedará limitado a casos de uso de bajo volumen, impidiendo su adopción generalizada y la materialización de sus promesas más transformadoras (Rao et al., 2024).

1.4. Objetivos del trabajo

El presente TFM persigue la consolidación y el análisis crítico de un campo tecnológico en constante evolución. Para ello, se establecen los siguientes objetivos específicos:

1. *Establecer los fundamentos teóricos de la tecnología blockchain.* Antes de abordar la escalabilidad, es imperativo comprender sus cimientos. Este objetivo se centra en desglosar la arquitectura del ecosistema, los tipos de redes existentes y el papel crucial de los algoritmos de consenso, con especial atención al problema de los generales bizantinos y a la solución de Bitcoin, la PoW.

2. *Analizar en profundidad el problema de la escalabilidad.* Se definirá formalmente el concepto de escalabilidad en sistemas distribuidos. Se identificarán las métricas clave de rendimiento (throughput, latencia) y se analizará el marco teórico del trilema de la blockchain, explicando el compromiso entre descentralización, seguridad y rendimiento.

3. *Realizar una revisión sistemática y clasificación de las soluciones de escalado.* Este es el núcleo del trabajo. Se llevará a cabo un recorrido exhaustivo, desde los sistemas permisionados hasta las soluciones más avanzadas, clasificándolas según la taxonomía estándar de Capa 1 (L1) (on-chain) y L2 (off-chain), y analizando mecanismos como la optimización de bloques, el sharding y los rollup.

4. *Desarrollar un análisis comparativo de las soluciones.* Se definirán criterios de evaluación para comparar las distintas familias de soluciones. Los resultados se sintetizarán en una tabla comparativa y se discutirán para extraer conclusiones sobre la idoneidad de cada enfoque según el caso de uso.

5. *Identificar los desafíos abiertos y las futuras líneas de investigación.* Como culminación del análisis, se explorarán las fronteras actuales de la investigación, como la sinergia de la blockchain con la ciencia de datos y el machine learning, así como los desafíos del creciente ecosistema de L2.

1.5. Metodología

Para alcanzar los objetivos propuestos, este trabajo adopta una metodología de *revisión bibliográfica sistemática* y *análisis comparativo*, enfoque idóneo para un campo con una literatura significativa pero fragmentada. La investigación se basa en la

recopilación, síntesis y evaluación crítica de una amplia gama de fuentes: artículos de investigación revisados por pares, tesis doctorales, libros blancos técnicos y documentación oficial de proyectos. La búsqueda se ha centrado en bases de datos académicas como IEEE Xplore, ACM Digital Library y Scopus, utilizando palabras clave como "blockchain scalability", "layer 2", "sharding", "rollups" y "consensus protocols".

La búsqueda inicial permitió constatar la existencia de un número considerable de trabajos de tipo "survey" que cubrían objetivos similares a los planteados en esta investigación. Si bien se seleccionaron los más citados como punto de partida, se observó que estos tendían a ser también los menos recientes. En consecuencia, las técnicas más novedosas para mejorar la escalabilidad de estos sistemas no llegaban a describirse en detalle en dichos trabajos, lo que identificó una brecha relevante a cubrir.

Adicionalmente, al abordar las contribuciones más importantes de cada artículo localizado, su extensión y número resultaron ser inmanejables en el marco de un trabajo académico de 12 créditos a realizar por un solo investigador novel, como es el caso de un estudiante de máster. Por ello, se tomó la decisión estratégica de acotar el alcance del estudio. El enfoque se ha centrado en describir brevemente, pero con claridad, las técnicas fundamentales ya identificadas en los "surveys" publicados, y complementar dicha base con el análisis de aquellas soluciones más recientes que no fueron analizadas con detenimiento en los trabajos más citados. Con el fin de producir un documento de tamaño razonable y fácilmente abordable para su evaluación, no se ha pretendido ser exhaustivo en la presentación o citación de todos los sistemas o artículos relacionados con cada una de las técnicas identificadas.

El análisis de la información se articula en torno a los marcos conceptuales aceptados en la comunidad investigadora. La clasificación principal de las soluciones sigue la distinción entre L1 (on-chain) y L2 (off-chain), un modelo ampliamente utilizado para estructurar el debate (Rebello et al., 2024; Zhou et al., 2020). Para la evaluación técnica de cada solución, se aplica un marco multidimensional que considera criterios como el rendimiento (throughput, latencia), el impacto en la seguridad y la descentralización, y la eficiencia de capital, permitiendo así una comparación rigurosa y fundamentada.

Capítulo 2

Fundamentos de la tecnología blockchain

Para entender el problema de la escalabilidad, es esencial comprender primero los componentes que definen una blockchain.

2.1. ¿Qué es un sistema blockchain? El libro contable distribuido

En su nivel más fundamental, una blockchain es una instancia de la Tecnología de Registro Distribuido (DLT). La metáfora más útil es la de un "libro contable digital" que, a diferencia de los registros tradicionales mantenidos por una entidad central, es *distribuido*, *inmutable* y *transparente* (Hafid et al., 2020).

El carácter *distribuido* implica que no existe una copia maestra. En su lugar, cada participante de la red, o nodo, mantiene una réplica idéntica y completa del registro. Los nodos se comunican a través de una red P2P, sin necesidad de un servidor central. Cualquier nueva entrada o *transacción* se transmite a toda la red para su validación.

La *inmutabilidad* se logra mediante una ingeniosa estructura de datos. Las transacciones se agrupan en bloques, y cada nuevo bloque contiene una referencia criptográfica al que le precede: su hash. Un hash es una función que convierte cualquier dato en una cadena de longitud fija, de tal manera que un cambio mínimo en la entrada produce un hash completamente diferente. Al incluir el hash del bloque anterior, se crea una cadena secuencial. Si un actor malicioso alterara

una transacción pasada, el hash de ese bloque cambiaría, rompiendo la cadena de todos los bloques posteriores. Esta discrepancia sería inmediatamente detectada y rechazada por los demás nodos, haciendo la manipulación computacionalmente inviable (Nakamoto, 2008).

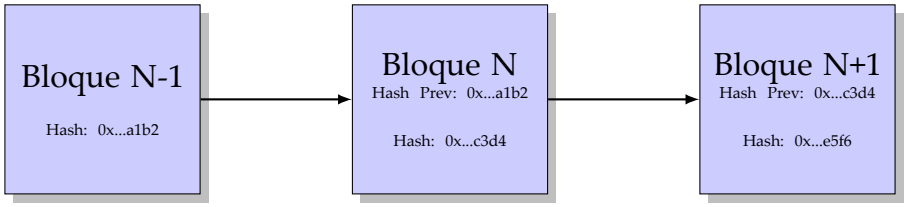

Figura 2.1: Estructura de una cadena de bloques.

Finalmente, para que un nuevo bloque se añada a la cadena, los nodos deben acordar su validez. Este proceso, conocido como algoritmo de consenso, es el corazón del sistema y el mecanismo que permite a una red de participantes sin confianza mutua llegar a un acuerdo sobre una única verdad compartida. La necesidad de este acuerdo coordinado, que se explorará en la sección 2.3.4, garantiza la integridad del libro contable, pero también es la principal fuente de sus limitaciones de rendimiento.

Blockchain es, por tanto, un sistema con propiedades emergentes de gran valor: *descentralización*, *seguridad*, *transparencia* y *auditabilidad*, convirtiendo a la tecnología en una nueva infraestructura para la confianza digital.

2.2. Arquitectura del ecosistema blockchain

Para comprender la tecnología blockchain, es útil descomponerla en capas lógicas que conforman el ecosistema. Uno de los modelos más aceptados es el de cinco capas propuesto por Sanka et al. (Sanka & Cheung, 2021), que abarca desde la infraestructura física hasta la interfaz de usuario.

2.2.1. Capa de plataforma (Platform Layer)

Es la capa más fundamental, que representa la *infraestructura de hardware y software base*. Incluye los componentes físicos de los nodos (servidores, almacenamiento) y, a nivel de software, el Sistema Operativo (SO) y el entorno de ejecución de cada contrato inteligente, cuyo ejemplo más prominente es la Máquina Virtual

de Ethereum (EVM), una máquina Turing-completa. La eficiencia de esta capa impone un límite físico al rendimiento del sistema.

2.2.2. Capa de red (Network Layer)

Esta capa es responsable de la *comunicación entre nodos* y gestiona los protocolos de comunicación P2P. Estos definen cómo los nodos se descubren, sincronizan el estado del libro contable y propagan nueva información mediante protocolos de "gossip". La latencia y el ancho de banda de esta capa son factores críticos que influyen en el tiempo de propagación de los bloques y, por tanto, en la seguridad y el rendimiento del sistema (Nasir et al., 2022).

2.2.3. Capa de consenso (Consensus Layer)

Es el núcleo lógico de la blockchain. Su función es *asegurar que todos los nodos lleguen a un acuerdo sobre una única versión de la historia*. Implementa el algoritmo de consenso (p. ej., PoW, Prueba de Participación (PoS)), que dicta las reglas para proponer, validar y resolver conflictos entre bloques. Dado que este proceso de coordinación global requiere comunicación y coste (computacional o económico), la capa de consenso es la principal fuente del cuello de botella de la escalabilidad (Rebello et al., 2024).

2.2.4. Capa de datos (Data Layer)

Define la *estructura de datos fundamental* de la cadena: el formato de las transacciones, la composición de los bloques y el mecanismo de encadenamiento mediante hashs. Una estructura clave en esta capa es el árbol de Merkle, que permite resumir todas las transacciones de un bloque en un único hash raíz (la *Merkle Root*). Esto posibilita la verificación eficiente de la inclusión de una transacción sin necesidad de descargar el bloque completo (Hafid et al., 2020).

2.2.5. Capa de aplicación (Application Layer)

Es la capa superior, la que interactúa con los usuarios. Engloba cada contrato inteligente y Aplicación Descentralizada (DApp). Un contrato inteligente es un programa autoejecutable desplegado en la red, mientras que la DApp es la interfaz

que permite a los usuarios interactuar con el. Ejemplos de esta capa incluyen los tokens fungibles (como los ERC-20 de Ethereum que alimentan el ecosistema de Finanzas Descentralizadas (DeFi)) y los Token No Fungible (NFT) (como los ERC-721 en Ethereum).

Figura 2.2: El modelo de cinco capas del ecosistema blockchain.

2.3. Taxonomía de sistemas blockchain

Los sistemas blockchain se clasifican según su modelo de gobernanza, principalmente en blockchain permisionadas y blockchain no permisionadas (*permissioned vs. permissionless*). Esta distinción determina quién puede participar, qué algoritmo de consenso es viable y, en última instancia, los compromisos del sistema frente al trilema de la blockchain. Comúnmente se dividen en tres categorías: públicas, privadas y de consorcio (Hafid et al., 2020).

2.3.1. Blockchains Públicas

Son redes abiertas y blockchain no permisionadas. Cualquier individuo puede unirse, participar en el consenso y auditar el libro contable sin aprobación de una autoridad central (Nakamoto, 2008). Este acceso abierto garantiza una *alta descentralización* y *resistencia a la censura*, pero requiere algoritmos de consenso computacionalmente intensivos como la PoW para protegerse de ataques. Este requisito es la causa directa de su *baja escalabilidad*.

- *Ejemplos:* Bitcoin, Ethereum, Litecoin.
- *Casos de uso:* Criptomonedas, sistemas que requieren máxima resistencia a la censura.

2.3.2. Blockchains Privadas

Son redes cerradas y blockchain permisionadas, controladas por una única organización que decide quién accede y con qué permisos. Al operar en un entorno de confianza, utilizan algoritmos de consenso más eficientes (variantes de Tolerancia a Fallos Bizantinos (BFT)), lo que les confiere una *alta escalabilidad* y rendimiento a costa de la *centralización*. Son, en esencia, bases de datos distribuidas con garantía de inmutabilidad.

- *Ejemplos:* Una implementación de Hyperledger Fabric para la logística interna de una empresa con múltiples sedes.
- *Casos de uso:* Aplicaciones empresariales donde la eficiencia prima sobre la descentralización.

2.3.3. Blockchains de Consorcio (o Federadas)

También blockchain permisionadas, se sitúan en un punto intermedio. Son gobernadas por un grupo preseleccionado de organizaciones, por lo que ninguna tiene el control total. Este modelo híbrido ofrece una *mayor descentralización* que una blockchain privada, pero mantiene una *alta escalabilidad* al usar algoritmos de consenso eficientes (Nasir et al., 2022). Son la opción preferida para la colaboración Empresa a Empresa (B2B).

- *Ejemplos:* Redes de cadena de suministro (p. ej., IBM Food Trust), redes de liquidación interbancaria.
- *Casos de uso:* Consorcios industriales y aplicaciones donde un grupo de entidades necesita un registro común.

2.3.4. El papel del consenso distribuido

El algoritmo de consenso es el protocolo que opera en la *Capa de Consenso* para garantizar que todos los nodos de una red distribuida mantengan una réplica idéntica y consistente del libro contable. Desde la perspectiva de la teoría de Sistemas

Distribuidos, el objetivo es lograr la propiedad de *replicación de máquinas de estado* (State Machine Replication), donde un conjunto de servidores deterministas comienzan en el mismo estado inicial y aplican la misma secuencia de operaciones, asegurando que sus estados finales permanezcan sincronizados.

El principal desafío reside en el modelo de fallos que el sistema puede tolerar. Ejemplos clásicos de algoritmo de consenso, como Paxos (Lamport, 2001) o Raft (Ongaro & Ousterhout, 2014), están diseñados para un modelo de Tolerancia a Fallos por Caída (CFT), donde los nodos pueden fallar deteniéndose, pero no se comportan de manera maliciosa. Las blockchains públicas, por ser sistemas abiertos donde podría haber adversarios, deben operar bajo un modelo de amenaza mucho más estricto: la BFT, donde los nodos pueden fallar de manera arbitraria, incluyendo el envío de información falsa o contradictoria para sabotear el consenso.

2.3.4.1. El problema de los generales bizantinos

El problema de los generales bizantinos, formalizado por Lamport, Shostak y Pease, es el modelo canónico de este desafío (Lamport et al., 1982). El problema demuestra que, para que un conjunto de n nodos alcance el consenso en un entorno asíncrono y en presencia de f nodos maliciosos (bizantinos), se debe cumplir la condición de que el número de nodos honestos sea estrictamente mayor que el doble de los nodos maliciosos ($n - f > 2f$), lo que se simplifica a $n > 3f$. En otras palabras, se requiere que más de dos tercios de los participantes sean honestos para garantizar la seguridad del sistema.

Esta condición matemática es inaplicable en una red pública y anónima. En un entorno así, un adversario puede ejecutar un ataque Sybil, creando un número arbitrario de identidades pseudónimas a un coste insignificante. Si el consenso se basara en contar identidades ("un voto por nodo"), un atacante podría superar fácilmente el umbral de $f = n/3$ y paralizar o corromper la red. Por lo tanto, el reto fundamental que Bitcoin debía resolver era diseñar un mecanismo de consenso BFT que fuera resistente a los ataques Sybil sin depender de un control de admisión centralizado.

2.3.4.2. Proof-of-Work (PoW): Consenso Nakamoto

La solución de Satoshi Nakamoto, conocida como Consenso Nakamoto, fue implementar un sistema BFT a través de un mecanismo de PoW (Nakamoto, 2008).

Su innovación no fue inventar PoW, sino recontextualizar el concepto de *Hashcash* de Adam Back (Back, 2002) como la piedra angular de un nuevo tipo de algoritmo de consenso. El mecanismo funciona de la siguiente manera: para proponer un nuevo bloque, los nodos "mineros" deben encontrar un valor (un *nonce*) tal que el hash criptográfico del encabezado del bloque sea inferior a un umbral de dificultad definido por el protocolo. Este proceso es computacionalmente costoso y probabilístico, pero su resultado es trivialmente verificable por cualquier otro nodo.

Este diseño resuelve el problema BFT en un entorno abierto de dos maneras fundamentales. Primero, proporciona una robusta *resistencia Sybil*: el poder de voto en la red no se deriva de la identidad, sino de un recurso externo, no falsificable y económicamente escaso: el poder computacional. El principio deja de ser "una identidad, un voto" para convertirse en "una CPU, un voto". Segundo, establece una *regla de selección de cadena objetiva*: la cadena canónica es siempre aquella con la mayor cantidad de Prueba de Trabajo acumulada (la más "pesada" o, comúnmente, la más larga). Un atacante que desee revertir una transacción tendría que recrear no solo el trabajo de ese bloque, sino el de todos los bloques posteriores a un ritmo superior al de toda la red honesta, un ataque del 51 % cuyo coste es prohibitivo.

PoW es, por tanto, un modelo de *replicación activa* que opera en un *entorno asíncrono*, sin embargo, su lentitud deliberada y su ineficiencia energética, características intrínsecas a su modelo de seguridad, lo convierten en el principal cuello de botella para la escalabilidad (Hafid et al., 2020; Rebello et al., 2024).

2.3.4.3. Alternativas a PoW: la búsqueda de la escalabilidad

Las limitaciones de PoW catalizaron la investigación de paradigmas de consenso alternativos, cada uno proponiendo un equilibrio distinto en el trilema de la blockchain.

La PoS sustituye la seguridad basada en el coste computacional por una seguridad basada en el coste de capital (Nasir et al., 2022). Los validadores bloquean una participación económica (*stake*) en la red. Para abordar el problema de "nada en juego" (un escenario en el que un validador, sin coste marginal por firmar, podría apoyar múltiples bifurcaciones competidoras, impidiendo el consenso), los sistemas PoS implementan un mecanismo de slashing. Si un validador firma un bloque contradictorio o ataca la red, una parte o la totalidad de su *stake* es destruida por el protocolo. Este fuerte desincentivo económico hace que la honestidad

sea la estrategia dominante y elimina la necesidad de un alto consumo energético, lo que permite un mayor rendimiento.

La Prueba de Participación Delegada (DPoS), introducida por Larimer (Larimer et al., 2014), optimiza el rendimiento sacrificando descentralización. En DPoS, los tenedores de tokens eligen mediante votación a un conjunto reducido y fijo de productores de bloques. Esta reducción del conjunto de validadores minimiza la sobrecarga de comunicación y la latencia del consenso, permitiendo alcanzar un alto número de TPS. Es un claro compromiso en el trilema, adecuado para aplicaciones que priorizan la velocidad sobre la máxima resistencia a la censura (Zhou et al., 2020).

Finalmente, los algoritmos de BFT clásicos, como el Tolerancia Práctica a Fallos Bizantinos (PBFT) de Castro y Liskov (Castro & Liskov, 1999), han sido adaptados para blockchain permisionadas. Estos protocolos se caracterizan por su finalidad determinista: una vez que un bloque es aprobado por la supermayoría requerida ($> 2/3$), es final e irreversible. Esto contrasta con la finalidad probabilística de PoW y PoS, donde la certeza de una transacción aumenta con cada bloque posterior pero nunca es absoluta. La alta complejidad de comunicación de los protocolos BFT, a menudo de orden O(n^2), los hace inviables para redes públicas con miles de nodos, pero su velocidad y finalidad inmediata los convierten en la solución idónea para los consorcios empresariales (Hafid et al., 2020).

Capítulo 3

El problema de la escalabilidad en blockchain

Una vez establecidos los fundamentos de la tecnología, es crucial analizar en profundidad el obstáculo más significativo para su adopción global: el problema de la escalabilidad. Este capítulo desglosa la naturaleza multidimensional de esta limitación. Se comenzará por establecer una definición formal de escalabilidad, anclada en la literatura clásica de sistemas distribuidos. A partir de este marco, se analizará cómo se mide y cómo debería medirse el trabajo en una red descentralizada, para luego explorar las causas raíz del problema a nivel de protocolo. Posteriormente, se analizarán las graves consecuencias sistémicas que emergen de estas limitaciones y se unificará todo bajo el modelo teórico del trilema de la blockchain, sentando las bases para comprender la urgencia y el enfoque de las soluciones que se analizarán en capítulos posteriores.

3.1. ¿Qué es realmente la escalabilidad? Una definición formal

El término escalabilidad se utiliza con frecuencia en la informática, pero su uso a menudo carece de rigor. Ya en 1990, Mark Hill advertía que, sin una definición formal, el concepto corría el riesgo de convertirse en una palabra vacía, más útil para el marketing que para el análisis técnico (Hill, 1990).

Una década más tarde, Jogalekar y Woodside propusieron una definición formal que abordaba esta carencia. Su contribución fundamental fue argumentar que la escalabilidad no puede evaluarse únicamente en términos de rendimiento (*th-*

roughput), sino que debe considerar también el coste económico y de recursos necesarios para alcanzarlo (Jogalekar & Woodside, 2000). Un sistema es verdaderamente escalable si, al aumentar la carga de trabajo, puede mantener un nivel de rendimiento aceptable de una manera costo-efectiva. Esta perspectiva dual (que une rendimiento y coste) es el prisma analítico a través del cual debe examinarse el problema en blockchain, donde el coste de la participación (y, por tanto, de la descentralización) es un factor primordial.

3.2. De la métrica tradicional (TPS) a la medida real del trabajo (Gas)

A la luz de la definición formal anterior, el debate sobre la escalabilidad en blockchain, a menudo simplificado al centrarse en una única métrica de rendimiento como las TPS, se revela inmediatamente como inadecuado. En blockchains de propósito general con capacidad de cómputo máquina Turing-completa como Ethereum, esta métrica es engañosa y, lo que es más importante, ignora por completo la dimensión del coste que Jogalekar y Woodside (2000) identificaron como esencial. El concepto de transacción no representa una unidad de trabajo estandarizada; existe una disparidad computacional abismal entre una simple transferencia de valor y la ejecución de un contrato inteligente complejo con múltiples operaciones (Rebello et al., 2024).

La solución técnica a este problema de medición fue la introducción del concepto de gas en el protocolo de Ethereum, un principio hoy universalmente aceptado para cuantificar recursos en sistemas similares (Wood, 2014). El gas es una unidad abstracta que mide el coste de los recursos computacionales consumidos por una operación (CPU, almacenamiento, ancho de banda). Cada código de operación (opcode) de la EVM tiene un coste fijo en gas, lo que permite medir con precisión la carga real que una transacción impone sobre la red. Por tanto, la métrica pertinente, que sí se alinea con una visión rigurosa de la escalabilidad, no es el número de transacciones, sino la cantidad total de gas que la red puede procesar por segundo, pues esta cifra representa el verdadero rendimiento computacional ponderado por su coste.

3.3. Las causas raíz del problema a nivel de protocolo

Si la medida correcta del rendimiento es el gas por segundo, la pregunta fundamental es: ¿qué impide que la red procese una mayor cantidad? La respuesta reside en la propuesta de valor central de la tecnología: la descentralización, que impone dos restricciones críticas a cada nodo de la red para mantener bajo el coste de participación y verificación.

3.3.1. El límite de rendimiento: La barrera del límite de gas del bloque

La integridad de una blockchain pública se fundamenta en la verificación universal: la capacidad de que cualquier participante pueda verificar de forma independiente la totalidad de la historia transaccional. Para que esta propiedad sea significativa, el coste de operar un nodo debe permanecer bajo, accesible para hardware de consumo.

En consecuencia, el protocolo debe imponer un límite estricto a la cantidad de trabajo computacional que puede incluirse en cada bloque. Este límite se materializa en el parámetro conocido como el límite de gas del bloque. No es un límite arbitrario, sino la implementación técnica de una política socio-económica: el protocolo restringe deliberadamente su propio rendimiento para asegurar que los validadores con menos recursos puedan procesar los bloques a tiempo, mantenerse sincronizados y participar plenamente en el consenso, preservando así la descentralización de la red (Croman et al., 2016). Este límite es el cuello de botella inmediato que determina el rendimiento máximo de la red.

3.3.2. El límite de almacenamiento: La amenaza del crecimiento del estado

Más allá del límite en el trabajo computacional por bloque, existe una segunda dimensión, más silenciosa pero igualmente crítica, que restringe la escalabilidad a largo plazo: el crecimiento del estado. Este término se refiere al crecimiento continuo e inevitable del conjunto de datos del estado de la blockchain (la colección de todas las cuentas, saldos, y datos almacenados en el contrato inteligente) que los nodos completos deben mantener para poder procesar y validar nuevas transacciones (Rebello et al., 2024).

Cada nueva transacción que modifica una cuenta o un contrato inteligente contribuye a este crecimiento. En una red de alta actividad, el estado puede expandirse a un ritmo de varios gigabytes por año. Esto presenta una amenaza directa y existencial a la descentralización por varias razones:

- **Aumento de los requisitos de hardware:** Un estado grande exige discos de estado sólido (SSD) de alta velocidad y gran capacidad, así como una cantidad considerable de memoria RAM para un acceso eficiente. Con el tiempo, estos requisitos superan las capacidades del hardware de consumo.
- **Tiempos de sincronización más largos:** Para un nuevo nodo que se une a la red, descargar y verificar todo el historial para reconstruir el estado actual puede llevar días o incluso semanas, disuadiendo a nuevos participantes.

El crecimiento del estado es, por tanto, una bomba de relojería para la descentralización. A mayor uso de la red, más rápido crece el estado, y más se centraliza la validación en manos de aquellos que pueden permitirse el coste del almacenamiento.

3.4. Consecuencias sistémicas y desafíos emergentes

Las restricciones fundamentales de rendimiento y almacenamiento, impuestas para preservar la descentralización a un coste razonable, no son meramente teóricas. Generan problemas en cascada que afectan a todo el ecosistema, creando un entorno hostil para los usuarios y desarrolladores.

3.4.1. Mercado de comisiones y valor extraíble (MEV)

El espacio en los bloques es un recurso escaso, y su asignación se rige por un mercado de subastas. Esta dinámica, una manifestación de la "Tragedia de los Comunes" (Hardin, 1968), genera dos problemas graves. Primero, la *volatilidad de las comisiones*: en picos de demanda, las tarifas se vuelven impredecibles, llegando a costes prohibitivos. Segundo, y más perverso, el Valor Máximo Extraíble (MEV), que fue formalizado por Daian et al. (2020). Dado que los productores de bloques controlan el orden de las transacciones, pueden reordenarlas, insertarlas o censurarlas para obtener un beneficio a costa de los usuarios, a través de estrategias como el ataque de anticipación. La escalabilidad limitada exacerba el MEV, al intensificar la competencia por el espacio y hacer más valioso el poder del productor de bloques.

3.4.2. La latencia de finalidad

Es crucial distinguir entre la latencia de inclusión (tiempo para que una transacción entre en un bloque) y la finalidad (tiempo hasta que se considera irreversible). Para aplicaciones del mundo real como los pagos, solo importa la finalidad. En PoW, esta puede ser de una hora para obtener alta confianza, ya que los bloques pueden ser reorganizados (Karame et al., 2012). En PoS, aunque más rápida, aún puede requerir varios minutos. Esta alta latencia de finalidad, una consecuencia directa de los consensos diseñados para redes globales, es un obstáculo fundamental para competir con sistemas de pago centralizados, que ofrecen finalidad en segundos.

3.4.3. Fragmentación y riesgos de los puentes

Paradójicamente, la proliferación de soluciones al problema de la escalabilidad, como las cadenas alternativas y las soluciones de L2, ha creado un nuevo problema: la *fragmentación del ecosistema*. La liquidez y los usuarios están divididos en silos incomunicados. Para mover activos entre ellos, se deben usar puentes. Estos componentes, aunque cruciales para la interoperabilidad, han demostrado ser el eslabón más débil del ecosistema, sufriendo algunos de los mayores hackeos de la historia debido a su complejidad y a los riesgos inherentes de su diseño (Zamyatin et al., 2019).

3.5. Formalización del conflicto: El trilema de la blockchain

Este complejo entramado de causas (límites de protocolo) y efectos (altas comisiones, MEV, mala experiencia de usuario) puede entenderse de manera unificada a través de un poderoso modelo conceptual: el trilema de la blockchain, popularizado por Vitalik Buterin (Buterin, 2017). Describe la tensión inherente entre el objetivo de procesar más trabajo computacional (*escalabilidad*) y la necesidad de mantener bajo el coste de la verificación (en términos de procesamiento, almacenamiento y participación) para proteger la *descentralización* y, por extensión, la *seguridad*.

El trilema postula que cualquier intento de mejorar una de estas propiedades tiende a degradar al menos una de las otras dos. Por ejemplo, un aumento sustancial

del límite de gas del bloque para mejorar la *escalabilidad* incrementaría los requisitos de hardware y aceleraría el crecimiento del estado. Esto aumentaría el coste de la validación, lo que llevaría a una mayor *centralización*. Una red más centralizada, con un número menor de validadores, reduce la robustez del consenso y el coste teórico de un ataque del 51 %, comprometiendo así la *seguridad*.

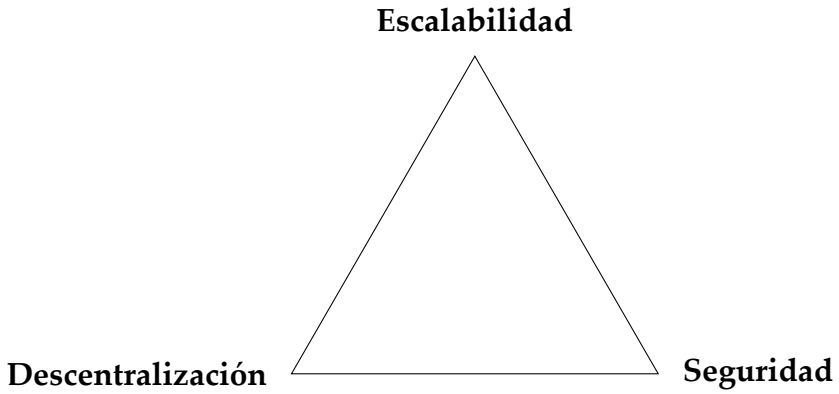

Figura 3.1: Representación visual del Trilema de la Blockchain como la formalización de la tensión entre escalabilidad y el coste de la verificación descentralizada.

3.6. Conclusión: La escalabilidad como un problema de eficiencia en la verificación

Del análisis anterior se desprende una conclusión fundamental: el problema de la escalabilidad en blockchain no es un problema de rendimiento bruto, sino de la *eficiencia del mecanismo de verificación*. Volviendo a la definición formal de Jogalekar y Woodside (2000), el desafío no es solo aumentar el rendimiento, sino hacerlo sin que el coste de la verificación individual se dispare hasta el punto de destruir la descentralización. Si la restricción fundamental es el requisito de que cada nodo verifique cada operación y almacene cada estado, entonces las soluciones de escalado deben ser entendidas como innovaciones en el paradigma de la verificación.

Las estrategias que se explorarán en los siguientes capítulos pueden, por tanto, ser clasificadas según cómo modifican este paradigma. Las soluciones de **L1**, como el sharding, proponen un modelo de *verificación dividida* o paralela. Las soluciones de **L2**, como los rollup, proponen un modelo de *verificación delegada*, donde la ejecución se externaliza. En última instancia, el progreso en la escalabilidad no reside en el incremento de la potencia computacional bruta, sino en la innovación de los métodos mediante los cuales se proporcionan garantías criptográficas sobre

la integridad de la computación realizada, reduciendo la carga impuesta a cada validador individual.

Capítulo 4

Soluciones de escalado: Un recorrido tecnológico

Frente al problema de la escalabilidad, conceptualizado en el capítulo anterior como un desafío multifacético que abarca desde los límites del protocolo hasta las consecuencias sistémicas, han surgido múltiples líneas de investigación. Las soluciones propuestas se pueden clasificar, de forma general, en dos categorías principales según dónde se implementa la mejora: en la propia cadena de bloques (on-chain o Capa 1) o en un protocolo que opera sobre ella (off-chain o Capa 2). Este capítulo realizará un recorrido tecnológico exhaustivo a través de estas soluciones, comenzando por la primera y más pragmática respuesta histórica al problema del rendimiento: el desarrollo de los sistemas permisionados, para luego adentrarse en las innovaciones para redes públicas.

4.1. Primera solución histórica: los sistemas permisionados

A medida que la tecnología blockchain trascendió el ámbito de las criptomonedas y captó el interés del sector empresarial, sus características fundamentales se revelaron como barreras para su adopción. Las redes públicas como Bitcoin y Ethereum, diseñadas para una máxima descentralización y resistencia a la censura, presentaban serios inconvenientes para los casos de uso corporativos: un rendimiento transaccional insuficiente, una finalidad con alta latencia, la ausencia total de privacidad de los datos y un modelo de gobernanza inexistente o caótico.

La primera "solución" al problema de la escalabilidad, por tanto, no surgió como

una optimización de estos sistemas abiertos, sino como una reimaginación fundamental de su arquitectura. En lugar de intentar escalar una red anónima, se optó por construir redes donde la confianza se gestiona a través de un estricto control de acceso. Nacieron así las DLT permisionadas, también conocidas como blockchains empresariales o de consorcio (Nasir et al., 2022).

La innovación central de un sistema permisionado es la sustitución del modelo de confianza anónimo por un modelo basado en la identidad. La participación en la red está restringida a un conjunto de actores autorizados por un Proveedor de Servicios de Membresía (MSP), como se denomina en arquitecturas como Hyperledger Fabric (Androulaki et al., 2018). Esta capa de identidad resuelve de raíz el ataque Sybil, eliminando la necesidad de recurrir a los lentos y costosos mecanismos de consenso como PoW. En su lugar, se emplean algoritmos de consenso deterministas y eficientes, como las variantes de BFT o incluso CFT como Raft, que permiten alcanzar la finalidad en segundos y procesar miles de TPS (Hafid et al., 2020).

Analizado desde la perspectiva del trilema de la blockchain, el enfoque permisionado no "resuelve" el trilema, sino que opera en un espacio de diseño diferente. Realiza un compromiso explícito: sacrifica la descentralización abierta a cambio de obtener una escalabilidad masiva, privacidad transaccional y una gobernanza clara. Su estudio es un punto de partida crucial, pues ilustra la relación directa entre el modelo de confianza de una red y su capacidad de rendimiento.

El ejemplo más representativo de esta arquitectura es Hyperledger Fabric. Impulsado por la Fundación Linux, fue diseñado con una arquitectura modular que permite a las empresas configurar redes privadas a través de "canales", aislando las transacciones entre los participantes pertinentes. En lugar de un consenso global, Fabric utiliza un flujo de 'ejecutar-ordenar-validar' donde los nodos de confianza (peers) ejecutan las transacciones, un servicio de ordenación (ordering service) las agrupa en bloques y finalmente los peers validan y confirman los cambios en sus respectivos libros contables (Androulaki et al., 2018).

4.2. Soluciones en la cadena (Capa 1 - On-Chain)

Las soluciones de escalado on-chain o de L1 representan el enfoque más fundamental para mejorar la capacidad de una red blockchain, ya que implican la modificación directa de las reglas del protocolo que rigen las capas de consenso y de datos. Estas estrategias buscan optimizar la forma en que los nodos procesan,

validan y almacenan la información, abordando directamente el cuello de botella que impone la verificación universal (Rebello et al., 2024). Su implementación es inherentemente compleja y a menudo controvertida (pues puede requerir bifurcaciones de la red (hard forks) y un amplio consenso comunitario), pero su impacto es profundo, ya que elevan el límite de rendimiento base sobre el cual pueden operar todas las aplicaciones y soluciones de L2.

4.2.1. Aumento del rendimiento del bloque

La forma más intuitiva de aumentar el rendimiento es permitir que cada bloque contenga más trabajo computacional. El método para lograrlo, sin embargo, tiene implicaciones críticas para la salud y la descentralización de la red.

4.2.1.1. Incremento del tamaño o límite de gas del bloque

La solución más directa y simple en apariencia es aumentar el tamaño máximo de los bloques (como en Bitcoin) o el límite de gas del bloque (como en Ethereum). Esta propuesta, defendida por proyectos como Bitcoin Cash, permite un incremento lineal de las TPS. No obstante, esta estrategia es ampliamente criticada por sus efectos secundarios sobre la descentralización. Un mayor tamaño de bloque exige más recursos de hardware (CPU para validación, almacenamiento para el historial y ancho de banda para la propagación) a los nodos. Esto eleva la barrera de entrada para que usuarios comunes puedan operar un nodo validador, incentivando una peligrosa centralización en manos de actores con mayores recursos económicos. Un número menor de nodos validadores no solo reduce la resiliencia de la red, sino que también disminuye el coste teórico para ejecutar un ataque del 51 %, comprometiendo así la seguridad (Croman et al., 2016). Además, esta táctica acelera el problema del crecimiento del estado, el crecimiento insostenible del conjunto de datos del estado que los nodos deben mantener, lo que amenaza la viabilidad de la red a largo plazo.

Esta filosofía se materializó con la creación de Bitcoin Cash. En 2017, una facción de la comunidad de Bitcoin ejecutó una bifurcación dura (hard fork) para crear una nueva cadena. La modificación fundamental fue el aumento del límite del tamaño del bloque de 1 MB a 8 MB, con el objetivo de escalar la red para servir como un sistema de efectivo electrónico de bajo coste, una implementación directa de esta estrategia de escalado (Bitcoin Cash, 2017).

4.2.1.2. Optimización de la estructura de datos: segregated witness (SegWit)

Una aproximación más sofisticada y elegante es mejorar la eficiencia del espacio dentro de los límites existentes. La implementación canónica de esta filosofía es *Segregated Witness* (SegWit), una actualización de Bitcoin que reorganizó la estructura de las transacciones. Su innovación clave fue separar los datos de la firma digital ("el testigo" o *witness*) del resto de la información transaccional. En lugar de un simple límite de tamaño, SegWit introdujo el concepto de "peso de bloque" (*block weight*), asignando un menor peso a los datos de las firmas, que pueden ocupar una parte significativa del espacio. Esto permitió, de facto, que más transacciones cupieran en un bloque sin alterar el límite fundamental de 1 MB. Igualmente importante fue que SegWit solucionó un error de diseño conocido como "maleabilidad de las transacciones" (donde el ID de una transacción podía ser alterado sin invalidarla), un prerrequisito técnico indispensable para el desarrollo seguro de soluciones de L2 como la Lightning Network (Croman et al., 2016).

Esta solución fue implementada en la red Bitcoin en 2017. A diferencia de un cambio en el tamaño del bloque, se introdujo mediante una bifurcación suave (soft fork) retrocompatible, tal como se especifica en la Propuesta de Mejora de Bitcoin 141 (bip-141). Esta implementación permitió a la red aumentar su capacidad de forma efectiva sin forzar una división de la cadena (Lombrozo et al., 2015).

4.2.2. Evolución de los paradigmas de consenso

El algoritmo de consenso PoW es, por diseño, el principal factor limitante debido a su deliberada lentitud para garantizar la seguridad en un entorno anónimo. Por ello, la investigación se ha centrado en paradigmas que desvinculan la seguridad del consumo energético masivo, permitiendo una mayor velocidad.

4.2.2.1. Proof-of-stake (PoS)

El cambio a PoS es la estrategia de L1 más transformadora de los últimos años. En lugar de la seguridad basada en el trabajo computacional del PoW, el PoS se fundamenta en la seguridad económico-criptográfica. Los validadores deben depositar un capital significativo (*stake*) como garantía. Si actúan de forma maliciosa (por ejemplo, validando al mismo tiempo dos registros que se contradicen), su capital es parcial o totalmente destruido por el protocolo mediante un mecanismo

de slashing. Este fuerte desincentivo económico alinea sus intereses con la salud de la red y proporciona una solución elegante al problema de ”nada en juego”, el problema teórico donde los validadores no tendrían nada que perder al apoyar múltiples cadenas a la vez (Nasir et al., 2022).

Esta desvinculación del trabajo computacional intensivo permite tiempos de bloque mucho más cortos y regulares, lo que aumenta directamente el rendimiento. Además, los sistemas PoS pueden ofrecer una finalidad más rápida y determinista. A diferencia de la finalidad probabilística del PoW, donde la certeza de una transacción aumenta con cada nuevo bloque pero nunca es absoluta, muchos protocolos PoS (como el de Ethereum) incorporan rondas de votación que declaran los bloques como irreversibles una vez que una supermayoría (generalmente 2/3) de los validadores los ha atestiguado. Esto mejora drásticamente la experiencia de usuario para las DApp que requieren confirmaciones rápidas y seguras (Rebello et al., 2024).

El caso de estudio más significativo es el de Ethereum. Tras años de desarrollo, la red completó su transición de PoW a PoS en 2022, en el evento “The Merge”. Este proceso, formalizado en la Propuesta de Mejora de Ethereum 3675 (Propuesta de Mejora de Ethereum (EIP)-3675), reemplazó a los mineros por validadores. El nuevo mecanismo de consenso, Gasper, sentó las bases para futuras mejoras de escalabilidad al permitir tiempos de bloque más rápidos y una finalidad determinista (Kalinin et al., 2021).

4.2.2.2. Delegated proof-of-stake (DPoS)

Introducido por Daniel Larimer en el contexto de BitShares (Larimer et al., 2014), la DPoS es una variante de PoS optimizada para un alto rendimiento mediante un compromiso explícito en el trilema de la blockchain. En lugar de permitir que cualquier poseedor de *stake* pueda ser validador, el sistema funciona como una democracia representativa: los tenedores de tokens votan para elegir a un número reducido y fijo de productores de bloques (p. ej., 21 en la red EOS). Este pequeño comité puede alcanzar el consenso con una latencia mínima, ya que la sobrecarga de comunicación es drásticamente menor que en una red con miles de validadores. Esto permite que la red procese miles de TPS, pero a costa de una mayor centralización y una menor resistencia a la censura, ya que atacar o cooptar a un pequeño grupo de delegados es teóricamente más factible (Zhou et al., 2020).

La red EOS es la implementación canónica de este modelo. Fue diseñada desde cero para maximizar el rendimiento, tal como se describe en su libro blanco fun-

dacional. Permite a los poseedores de tokens elegir a 21 productores de bloques, que son responsables de crear los bloques en rondas predefinidas, lo que permite alcanzar tiempos de bloque de 0.5 segundos y sustituir las comisiones por transacción por un modelo de recursos basado en el stake (Larimer, 2017).

4.2.3. Optimización de la capa de ejecución

Más allá del consenso y el almacenamiento de datos, la propia eficiencia de la computación on-chain es un factor limitante. El trabajo computacional en Ethereum y cadenas compatibles se mide en gas, y el coste de cada opcode en la EVM determina cuánta lógica puede ejecutarse dentro del límite de gas del bloque. Por tanto, optimizar el entorno de ejecución es una vía directa para escalar la capacidad computacional de la L1. Las principales líneas de investigación en esta área incluyen:

- *Máquinas virtuales paralelizables:* La EVM es, en gran medida, de hilo único (single-threaded), lo que dificulta aprovechar el hardware moderno multinúcleo. Proyectos como Solana han diseñado su arquitectura desde cero para permitir la ejecución paralela de transacciones, siempre que estas no afecten al mismo estado. Esto permite un aumento drástico del rendimiento, aunque requiere que los desarrolladores estructuren sus DApp de forma explícita para indicar qué partes del estado van a modificar (Yakovenko, 2018).

- *Adopción de WebAssembly (WASM):* Varias blockchains de nueva generación (como Polkadot o Dfinity) han abandonado la EVM en favor de WASM. WASM es un estándar de la industria, diseñado por gigantes como Google, Mozilla y Microsoft, para ofrecer un rendimiento cercano al nativo. Sus ventajas en el contexto blockchain son una mayor eficiencia de ejecución (lo que se traduce en un menor coste de gas para operaciones complejas), soporte para más lenguajes de programación (como Rust y C++) y un ecosistema de herramientas mucho más maduro.

- *Precompilaciones y aceleración por hardware:* Para operaciones criptográficas muy costosas y repetitivas (como las necesarias para los ZK-Rollups), las blockchains pueden introducir "precompilaciones". Estas son implementaciones de funciones complejas a nivel de protocolo, escritas en código nativo y mucho más eficientes que su equivalente en la EVM. El siguiente paso lógico, aunque aún en fase de investigación, sería la aceleración por hardware, utilizando FPGAs o ASICs para procesar estas operaciones a velocidades

órdenes de magnitud superiores.

4.2.4. Paralelización del procesamiento: sharding y DAG

La solución más ambiciosa a nivel de L1 consiste en abandonar el modelo de procesamiento secuencial, donde cada nodo debe ejecutar cada transacción, y adoptar un modelo de "divide y vencerás".

4.2.4.1. Sharding

El sharding particiona la base de datos y la carga de trabajo de la red en múltiples cadenas más pequeñas, o *shards*, que operan en paralelo. En teoría, esto multiplica la capacidad de la red por el número de *shards* (Yu et al., 2020). Sin embargo, su implementación segura es uno de los mayores desafíos en sistemas distribuidos, presentando problemas como:

- *Seguridad y composición de los shards:* Para evitar que un atacante concentre su poder en un único *shard* (un "ataque del 1 %"), los validadores deben ser asignados aleatoria y periódicamente a los *shards*, lo que requiere una fuente segura y no manipulable de aleatoriedad en el propio protocolo.
- *Disponibilidad de datos (Data Availability):* Para que la red global sea segura, los nodos deben poder verificar que los datos de todos los *shard* se han publicado correctamente. Demostrar esta disponibilidad sin obligar a cada nodo a descargar todos los datos es un problema criptográfico complejo, fundamental para la seguridad de los rollup que dependen de la L1.
- *Comunicación y atomicidad cross-shard:* Garantizar que las transacciones que involucran a múltiples *shards* se ejecuten de forma atómica (o todo o nada) requiere complejos protocolos de comunicación y coordinación que añaden una sobrecarga significativa.

Este cambio de enfoque, ejemplificado por la EIP-4844 (Proto-Danksharding), es la manifestación más clara de la *Tesis de la Blockchain Modular*. Esta tesis postula que las blockchains monolíticas, que intentan hacerlo todo (consenso, disponibilidad de datos y ejecución), están fundamentalmente limitadas por el trilema de la blockchain. El futuro del escalado reside en la especialización:

- La *capa de ejecución* se traslada a las soluciones de L2 (rollups), que pueden procesar transacciones a gran escala.

- La *capa 1* se especializa en las tareas que solo ella puede hacer de forma descentralizada y segura:
    - *Consenso:* Proveer seguridad a toda la pila a través de su mecanismo (p. ej., PoS).
    - *Asentamiento (Settlement):* Actuar como el tribunal final donde se resuelven las disputas y se anclan los estados de las L2.
    - *Disponibilidad de datos:* Ofrecer un espacio de bajo coste y alta seguridad para que las L2 publiquen sus datos, garantizando que cualquiera pueda verificar el estado del rollup.

Por tanto, el sharding en su forma moderna, como el introducido en la EIP-4844 (Buterin et al., 2022), no es una alternativa a los rollups, sino su principal catalizador y aliado, al reducir drásticamente el coste de publicar datos en la L1 a través de *blobs* temporales en lugar del costoso calldata.

La hoja de ruta de Ethereum es el ejemplo más relevante de este enfoque. La implementación de la EIP-4844 (Proto-Danksharding) en 2024 introdujo un nuevo tipo de transacción para "blobs" de datos. Esto creó un mercado de datos separado y de bajo coste, diseñado específicamente para que las soluciones de Capa 2 publiquen sus datos, materializando el primer paso de la tesis modular (Buterin et al., 2022).

4.2.4.2. Estructuras de grafo acíclico dirigido (DAG)

Como una alternativa radical a la estructura secuencial de la blockchain, los sistemas basados en un Grafo Acíclico Dirigido (DAG) proponen un modelo donde las transacciones se procesan de forma asíncrona y paralela. El proceso de validación, ilustrado en la Figura 4.1, es fundamental para entender su funcionamiento. En lugar de agruparse en bloques, cada nueva transacción participa activamente en la seguridad de la red.

Como se observa en la figura, la red contiene transacciones ya confirmadas (en gris) y transacciones en espera de validación, conocidas como *'puntas'* o *'tips'* (en azul). Para que una nueva transacción (T_{Nueva}, en rojo) sea aceptada, debe realizar los siguientes pasos:

1. Seleccionar dos o más *'puntas'* de la red (en el ejemplo, T_A y T_B).

2. Verificar el historial de estas puntas para asegurar que no contienen conflictos, como un problema del doble gasto.

3. Emitir la nueva transacción, la cual incluye referencias (enlaces) que apuntan a las puntas que ha validado.

Con este acto, T_{Nueva} confirma explícitamente a T_A y T_B, integrándose en el grafo y convirtiéndose, a su vez, en una nueva punta a la espera de ser validada por transacciones futuras. Este mecanismo permite un alto rendimiento al eliminar el cuello de botella del tiempo de bloque.

Sin embargo, esta concurrencia introduce un desafío clave: establecer un ordenamiento total y definitivo de las transacciones. Para resolver esta ambigüedad, muchos proyectos recurren a nodos especiales —denominados *'coordinadores'*— que actúan como una autoridad centralizada para fijar el orden final. El proyecto IOTA y su arquitectura Tangle son un ejemplo paradigmático de este dilema: para garantizar la finalidad, la red dependió durante años de un *'Coordinador'* centralizado, ilustrando el sacrificio de la descentralización a cambio de seguridad (Popov, 2018).

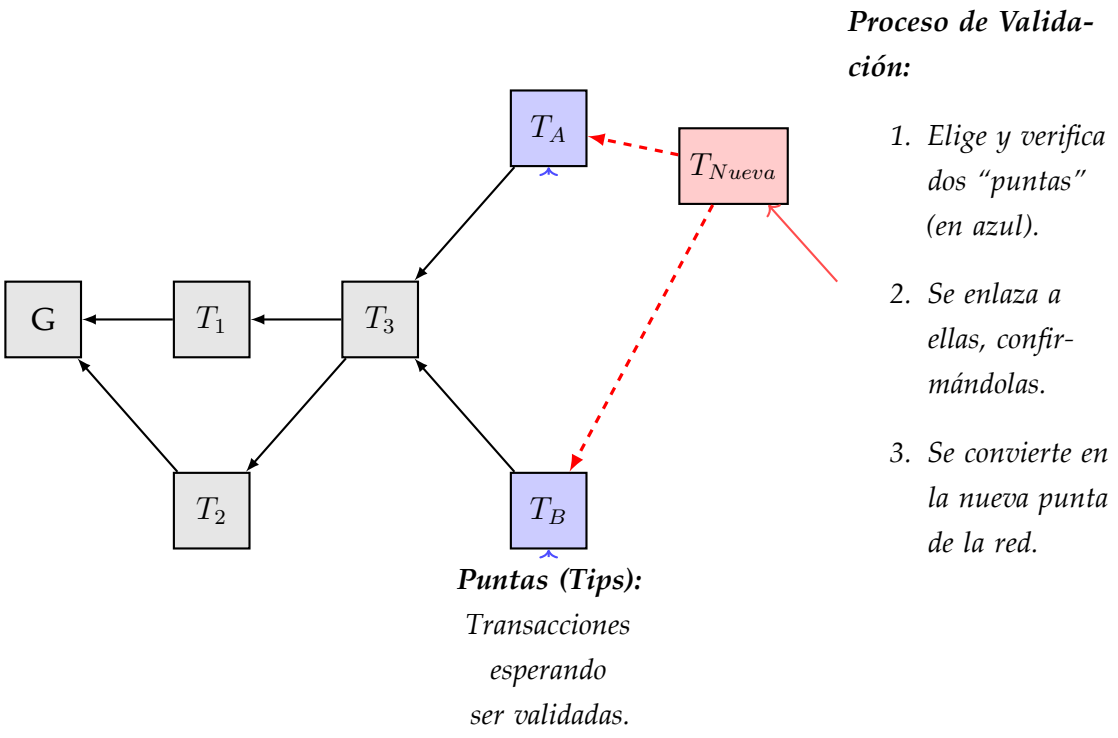

Figura 4.1: Visualización del proceso de validación en un DAG. La nueva transacción (T_{Nueva}) debe seleccionar y verificar dos transacciones no confirmadas (las "puntas" T_A y T_B) y enlazarse a ellas. Al hacerlo, las confirma y se integra en el grafo, esperando a su vez ser validada por transacciones futuras.

4.2.5. Gestión del estado a largo plazo: clientes sin estado

Un desafío fundamental que subyace a todas las soluciones de escalado es el del crecimiento del estado. A medida que la actividad de la red crece, también lo hace el conjunto de datos del estado (balances de cuentas, código de contratos, almacenamiento) que los nodos deben mantener para validar nuevas transacciones. Si este estado crece indefinidamente, el coste de operar un nodo se volverá prohibitivo para la mayoría, llevando inevitablemente a la centralización. La solución a largo plazo para este problema existencial es el concepto de "cliente sin estado".

La idea de la validación sin estado consiste en romper el requisito de que los validadores deban almacenar el estado completo de la red. En su lugar, las transacciones vendrían acompañadas de una prueba "criptográfica" (como un árbol de Merkle) que demuestra qué partes del estado necesita modificar y que el estado actual es el correcto. El validador solo necesitaría verificar esta prueba, sin necesidad de consultar una base de datos local. Este es el "santo grial" de la escalabilidad de L1 por dos razones:

1. *Permite una validación con recursos mínimos:* Un validador podría operar con un hardware muy modesto, reforzando masivamente la descentralización.

2. *Soluciona el problema del crecimiento del estado:* Si los validadores no necesitan el estado, su crecimiento deja de ser una amenaza directa para la participación en el consenso.

Implementar un modelo puramente sin estado es un desafío técnico inmenso. Un paso intermedio es el "vencimiento del estado" (*state expiry*), donde partes del estado que no se han utilizado durante un largo período se archivan, pudiendo ser reactivadas mediante una transacción especial. Estas ideas, aunque complejas, son la frontera de la investigación en L1 y la única solución conocida para garantizar la sostenibilidad y descentralización de las blockchains a escala de décadas.

A día de hoy, esta es una línea de investigación activa, y la hoja de ruta de Ethereum es el ejemplo más claro de su búsqueda. El trabajo se centra en la transición a los Árboles de Verkle, que permiten la generación de pruebas criptográficas mucho más pequeñas, un prerrequisito técnico fundamental para alcanzar la validación sin estado (Buterin, 2021).

4.3. Soluciones fuera de la cadena (Capa 2 - Off-Chain)

Si las soluciones on-chain intentan ensanchar la carretera, las estrategias de L2 u off-chain construyen un sistema de autopistas de alta velocidad que corren en paralelo. No modifican el protocolo de la blockchain principal. En su lugar, construyen un sistema secundario que opera "encima" de la L1, externalizando la gran mayoría del trabajo computacional. La L1 se utiliza de forma mínima, pero para lo que es indispensable: actuar como un *ancla de seguridad* y un *tribunal de última instancia* para resolver disputas y liquidar fondos. Este enfoque permite un aumento masivo del rendimiento, a menudo de órdenes de magnitud, sin comprometer la descentralización de la capa base.

4.3.1. Anatomía de una solución de capa 2: un marco general

Aunque existen múltiples diseños, el paradigma dominante, especialmente el de los rollup, sigue un ciclo de vida operativo común. Entender este flujo es fundamental para comprender los componentes, los actores y los compromisos de cada tecnología. A continuación, se describe el ciclo de vida de una transacción típica en una L2 moderna, introduciendo la terminología clave.

4.3.1.1. Etapa 1: depósito y ejecución off-chain

El proceso se inicia cuando un usuario deposita activos de la L1 en el contrato inteligente del puente de la L2. Una vez en la Capa 2, las transacciones se envían a un área de espera conocida como *mempool*. Desde allí, un actor clave, el *secuenciador* (*sequencer*), las selecciona, las ordena para formar un lote (*batch*) y las ejecuta.

Este poder para ordenar transacciones no es neutral y tiene profundas implicaciones económicas, dando lugar al fenómeno del *MEV*. En su estado actual, la mayoría de las L2 operan con un secuenciador centralizado. Esto representa el principal punto de confianza y el desafío más significativo a resolver, un punto crítico que se explorará en detalle en el capítulo 6.

4.3.1.2. Etapa 2: asentamiento y disponibilidad de datos on-chain

Tras la ejecución, el secuenciador debe anclar el resultado en la L1 para heredar su seguridad. Para ello, publica una única transacción en la L1 que contiene dos

elementos cruciales:

1. *Datos de la transacción:* los datos brutos del lote, generalmente en un formato muy comprimido. Su publicación en la L1 garantiza la *disponibilidad de datos*, un principio de seguridad que permite a cualquiera verificar el estado y asegura que los usuarios puedan retirar sus fondos incluso si el secuenciador falla.

2. *Prueba de la transición de estado:* una prueba que demuestra que el nuevo estado de la L2 es el resultado correcto de ejecutar las transacciones. Aquí es donde los diseños de L2 divergen fundamentalmente:

    - *Prueba de fraude (modelo optimista):* se asume que el estado es válido a menos que un observador presente una prueba criptográfica del fraude durante un período de disputa.

    - *Prueba de validez (modelo ZK):* en lugar de asumir la validez, este modelo la *demuestra*. Cada lote se publica junto a una prueba criptográfica (como un Argumento de Conocimiento Sucinto y No Interactivo (SNARK) o Argumento de Conocimiento Escalable y Transparente (STARK)) que certifica matemáticamente la validez de la transición de estado.

4.3.1.3. Etapa 3: retirada

Finalmente, cuando un usuario desea mover sus fondos de vuelta a la L1, su solicitud se incluye en un lote. Una vez que este ha sido asentado y finalizado en la L1 (el período de disputa ha expirado o la prueba de validez ha sido verificada), el usuario puede retirar sus activos del contrato del puente.

Este marco general (depósito, ejecución off-chain, asentamiento en L1 y retirada) define la arquitectura de las soluciones de escalado más avanzadas. Las siguientes secciones analizarán cómo implementaciones específicas aplican, modifican o se desvían de este modelo.

4.3.2. Canales de estado: la vía rápida privada

El uso de un canal de estado es una de las primeras y más intuitivas soluciones de L2. El mecanismo funciona de la siguiente manera: dos o más participantes realizan una transacción inicial on-chain para desplegar un contrato inteligente que bloquea una cantidad de fondos, como si fuera un depósito de garantía. Una vez

el canal está "abierto", pueden intercambiar un número virtualmente ilimitado de transacciones off-chain entre ellos. Cada transacción es simplemente un mensaje firmado criptográficamente que contiene el nuevo estado (p. ej., el balance actualizado de cada uno) y un número de versión creciente. Para prevenir fraudes, si una de las partes intenta cerrar el canal en la L1 publicando un estado antiguo, la otra parte tiene un tiempo para presentar una transacción con un número de versión más reciente. El contrato inteligente en la L1 está programado para reconocer siempre el estado con el número de versión más alto, invalidando el intento de fraude (Poon & Dryja, 2016).

La Lightning Network de Bitcoin es la implementación más conocida. Si bien son extremadamente eficientes para micropagos, sus limitaciones son inherentes a su diseño:

- *Ineficiencia de capital:* Los fondos deben permanecer bloqueados y sin poder usarse para otra cosa durante toda la vida útil del canal.
- *Requisito de "Liveness":* Los participantes deben estar constantemente en línea para poder disputar a tiempo un cierre fraudulento.
- *Limitaciones para contratos complejos:* Su naturaleza punto a punto los hace poco adecuados para interacciones complejas y multiparte, como las que dominan el ecosistema de DeFi.

La Lightning Network es el ejemplo por excelencia. Su diseño técnico, presentado originalmente por Joseph Poon y Thaddeus Dryja, fue implementado sobre Bitcoin aprovechando la activación de SegWit. Permite a los usuarios abrir canales de pago entre ellos, donde solo las transacciones de apertura y cierre se registran en la cadena principal, permitiendo un escalado masivo para micropagos (Poon & Dryja, 2016).

4.3.3. Sidechains: el modelo de soberanía propia

Las sidechains son blockchains independientes y soberanas que corren en paralelo a una cadena principal. Su mecanismo de conexión se basa en un puente que implementa un sistema de "bloqueo y acuñación" (*lock-and-mint*). Cuando un usuario quiere mover activos de la L1 a la sidechain, bloquea sus tokens en un contrato inteligente del puente en la L1. El puente detecta este evento y acuña una cantidad equivalente de tokens representativos (envueltos o *wrapped*) en la sidechain.

La principal ventaja de las sidechains es su flexibilidad. Al poseer su propio algo-

ritmo de consenso (p. ej., PoS), pueden optimizarse para un alto rendimiento. Sin embargo, esta soberanía es su mayor debilidad: *no heredan la seguridad de la cadena principal*. La seguridad de los fondos depende enteramente de la honestidad de los validadores de la sidechain. Si estos son atacados o se confabulan, pueden robar los fondos bloqueados en el puente de la L1. Por tanto, utilizar una sidechain implica un supuesto de confianza explícito en un nuevo conjunto de actores.

El ejemplo más exitoso de esta arquitectura es la cadena Polygon PoS. Opera en paralelo a Ethereum y utiliza su propio conjunto de validadores. Aunque es independiente, se conecta a Ethereum a través de un puente y sus validadores envían "checkpoints" del estado de la sidechain a la L1. Esta arquitectura, descrita en su documentación oficial, le permite ofrecer un entorno compatible con la EVM a cambio de no heredar la seguridad completa de Ethereum para cada transacción (Polygon Team, 2024).

4.3.4. Rollups: escalado con la seguridad de la capa 1

Los rollup representan el paradigma de L2 más prometedor, pues logran escalar la ejecución mientras heredan por completo la seguridad de la L1. Su mecanismo se basa en dos pilares:

1. *Ejecución Off-Chain:* Un operador de rollup, llamado secuenciador, recibe transacciones de los usuarios, las ordena y las ejecuta fuera de la cadena.

2. *Publicación de Datos On-Chain:* El secuenciador agrupa o "enrolla" cientos de transacciones en un solo lote y publica los datos de este lote, de forma muy comprimida, en la L1.

Esta garantía de disponibilidad de datos es la piedra angular de su seguridad. Al tener los datos en la L1, cualquier persona puede reconstruir el estado del rollup y verificar su integridad. Esto permite una "salida forzada": si el secuenciador censura a un usuario, este puede usar los datos en la L1 para retirar sus fondos directamente. La diferencia fundamental reside en cómo demuestran que la ejecución off-chain fue correcta.

4.3.4.1. Optimistic rollups: confianza con verificación social

Los Optimistic Rollups operan bajo el principio de "inocente hasta que se demuestre lo contrario". El secuenciador publica un nuevo estado en la L1 junto con una

fianza, asumiendo "optimistamente" que ha actuado con honestidad. Para protegerse de fraudes, se abre un "período de disputa" (generalmente de una semana). Durante este tiempo, cualquier observador puede descargar los datos, re-ejecutar las transacciones y, si encuentra una discrepancia, presentar una prueba de fraude en la L1. El contrato del rollup en la L1 es el árbitro: ejecuta la prueba de fraude (que identifica la instrucción específica donde hubo el fallo) y, si es válida, revierte el estado fraudulento, confisca la fianza del secuenciador y recompensa al verificador.

- *Ventajas:* Son totalmente compatibles con la EVM, lo que facilita la migración de DApp existentes.
- *Desventajas:* La latencia de finalidad. Para retirar fondos, los usuarios deben esperar a que finalice el largo período de disputa, lo que perjudica la experiencia de usuario.

Arbitrum One es el ejemplo más destacado de esta tecnología. Su sistema de seguridad se basa en un mecanismo de prueba de fraude interactivo, descrito en su artículo fundacional. Si un estado es desafiado, el secuenciador y el retador participan en un "juego de bisección" que permite identificar de forma eficiente la instrucción exacta en disputa. Este proceso se verifica finalmente en la L1, minimizando el coste computacional para el árbitro (Kalodner et al., 2018).

4.3.4.2. ZK-rollups: verificación con pruebas matemáticas

Los ZK-Rollups (del inglés, Conocimiento Cero (ZK)) utilizan un enfoque proactivo: "culpable hasta que se demuestre lo contrario con criptografía". Junto con cada lote de transacciones, el secuenciador debe generar y publicar en la L1 una prueba de validez. Esta es una prueba criptográfica sofisticada (como un SNARK) que actúa como un "notario criptográfico": demuestra matemáticamente que el nuevo estado publicado es el resultado correcto de ejecutar el lote de transacciones. El contrato del rollup en la L1 solo tiene que realizar una única operación: verificar que la prueba es matemáticamente válida. Este proceso es computacionalmente muy ligero para la L1.

- *Ventajas:* La finalidad es casi instantánea. Una vez la prueba es verificada en la L1 (minutos), los fondos son seguros y retirables. Su seguridad se basa en la certeza de las matemáticas, no en la vigilancia de actores económicos.
- *Desventajas:* La generación de pruebas de ZK es computacionalmente intensiva para el secuenciador. Lograr la compatibilidad total con la EVM (una

"zkEVM") es un desafío técnico inmensamente complejo.

Un caso de estudio relevante es zkSync Era. Este ZK-Rollup utiliza pruebas ZK-SNARK para garantizar la validez de las transacciones. Su implementación aborda el desafío de la compatibilidad con la EVM a nivel de lenguaje: compila lenguajes como Solidity a un conjunto de instrucciones optimizado para la generación de pruebas ZK. Este enfoque, detallado en su documentación técnica, busca equilibrar la facilidad para los desarrolladores con el rendimiento del sistema de pruebas (Matter Labs, 2024).

4.3.5. El espectro de soluciones híbridas

Las soluciones de L2 no son categorías discretas, sino un espectro de compromisos, principalmente en torno a dónde se almacenan los datos.

Validium es una de estas variantes. Funciona como un ZK-Rollup (usan prueba de validez para garantizar la integridad computacional), pero su mecanismo de datos es diferente: no los publican en la L1. En su lugar, los datos son custodiados off-chain por un Comité de Disponibilidad de Datos (DAC). Esto reduce drásticamente los costes, pero introduce un nuevo supuesto de confianza: si el DAC retiene los datos, los usuarios no podrían construir la prueba necesaria para retirar sus fondos, que quedarían congelados, aunque no podrían ser robados gracias a las pruebas de validez (Ben DiFrancesco, 2020).

Otras arquitecturas históricas, como *Plasma* (Poon & Buterin, 2017), también mantenían los datos off-chain y se basaban en un modelo de prueba de fraude. Fueron un precursor intelectual importante, pero su complejo diseño, que exigía a los usuarios monitorizar la cadena y descargar grandes cantidades de datos para asegurar sus fondos, limitó su adopción práctica en favor del modelo más robusto y simple de los rollup.

El motor StarkEx de StarkWare es la implementación más conocida de Validium. Ha dado servicio a aplicaciones de alto volumen como el exchange de derivados dYdX. En esta arquitectura, las transacciones se procesaban off-chain y su validez se garantizaba con una prueba STARK publicada en Ethereum. Sin embargo, los datos de las transacciones eran gestionados por un Comité de Disponibilidad de Datos (DAC) de confianza. Esto permitió a dYdX alcanzar un rendimiento de miles de transacciones por segundo, a cambio de introducir ese supuesto de confianza en el DAC (StarkWare, 2024).

Capítulo 5

Análisis comparativo a través del trilema de la blockchain

5.1. El desafío metodológico de la comparación

El estudio de las soluciones de escalado, presentado en el capítulo anterior, revela un ecosistema tecnológico heterogéneo. Un análisis riguroso de estas soluciones enfrenta un desafío metodológico significativo: las diferentes arquitecturas no representan meras variaciones de una misma tecnología, sino paradigmas con objetivos y compromisos fundamentales distintos. Por tanto, una comparación directa sin un marco de evaluación unificado y contextualizado carecería de validez científica.

Este capítulo aborda dicho desafío mediante la aplicación de una metodología sistemática. Se utiliza el trilema de la blockchain como marco teórico para derivar un conjunto de criterios de evaluación cuantitativos y cualitativos. El objetivo no es determinar una solución absolutamente "superior", sino realizar un análisis comparativo que mapee el espacio de los compromisos de cada arquitectura.

El análisis se estructura en secciones que evalúan las soluciones dentro de categorías lógicamente consistentes. Se discutirán en detalle los resultados de cada comparación para, finalmente, sintetizar los hallazgos en una conclusión global sobre la convergencia del campo hacia arquitecturas modulares especializadas.

5.2. Metodología

Para garantizar una evaluación objetiva y reproducible, se establece un marco de nueve criterios, derivados de los tres ejes del trilema. Cada criterio se evalúa en una escala del 1 (deficiente) al 5 (excelente), donde una puntuación más alta indica una mayor optimización de dicha propiedad.

5.2.1. Eje 1: Escalabilidad

Este eje cuantifica la capacidad del sistema para procesar un alto volumen de transacciones de manera eficiente y a bajo coste.

- **Rendimiento (throughput):** Mide la capacidad máxima sostenida de procesamiento de operaciones de la red, expresada en transacciones por segundo. Una puntuación alta (5) denota una capacidad para procesar miles de TPSs, mientras que una baja (1) indica un rendimiento similar o inferior al de una L1 no escalada.
- **Latencia de finalidad:** Evalúa el tiempo transcurrido desde que una transacción es enviada hasta que se considera final e irreversible en el estado del sistema. Un 5 representa una finalidad casi instantánea (segundos), mientras que un 1 implica una latencia de horas o días.
- **Coste por transacción:** Analiza la eficiencia económica de las operaciones, midiendo las comisiones requeridas para su procesamiento. Un 5 corresponde a costes que tienden a ser marginales, permitiendo microtransacciones, mientras que un 1 representa costes prohibitivos que limitan el uso a casos de alto valor.

5.2.2. Eje 2: Seguridad

Este eje evalúa la robustez del sistema frente a ataques maliciosos y la minimización de los supuestos de confianza necesarios para su operación.

- **Modelo de seguridad:** Examina el origen y la fortaleza de las garantías de seguridad del sistema. La máxima puntuación (5) se otorga a soluciones que heredan íntegramente la seguridad criptoeconómica de una L1 pública y descentralizada. La mínima (1) corresponde a sistemas aislados que depen-

den de un modelo de confianza extrínseco, como la honestidad de un consorcio.

- **Resistencia a la pérdida de fondos:** Mide la capacidad del protocolo para proteger los activos de los usuarios, incluso bajo un ataque exitoso al consenso o la indisponibilidad de sus operadores. Un 5 implica la existencia de garantías criptográficas que impiden la sustracción de fondos, mientras que un 1 indica un riesgo de pérdida total o congelamiento permanente.

- **Supuesto de confianza clave:** Mide la robustez de un sistema estableciendo una jerarquía de confianza, donde la certeza de las pruebas criptográficas (5) es superior a la confianza en una mayoría de actores (2-3) y, fundamentalmente, a la dependencia de un solo actor (1).

5.2.3. Eje 3: Descentralización

Este eje mide la distribución del poder dentro de la red, su apertura a la participación y su capacidad para resistir la coerción o la censura.

- **Requisitos para la validación:** Evalúa la accesibilidad real para participar en el consenso, considerando tanto barreras políticas como tecnológicas. La puntuación máxima (5) se otorga a sistemas no permisionados con requisitos de hardware y capital bajos, permitiendo una participación amplia. La mínima (1) denota barreras críticas que centralizan el poder de facto, ya sea por un modelo permisionado que exige autorización de un tercero o por requisitos técnicos prohibitivos, como la dependencia de hardware especializado (ASICs).

- **Nivel de centralización:** Identifica componentes del sistema cuyo control recae en una o pocas entidades, comprometiendo la neutralidad de la red. Un sistema sin puntos únicos de fallo o control (ej. secuenciador, validador, gobernanza) obtiene un 5. Por el contrario, un 1 señala una dependencia crítica de un componente centralizado.

- **Resistencia a la censura:** Mide la garantía de que cualquier transacción válida será eventualmente procesada sin discriminación. Un 5 indica que la inclusión de transacciones es un derecho garantizado por el protocolo, mientras que un 1 denota la existencia de un control centralizado sobre el ordenamiento de transacciones que podría ser utilizado para censurar a los usuarios.

5.3. Análisis de las redes permisionadas

El análisis comienza con las redes permisionadas. Estas arquitecturas, al operar en un entorno con control de acceso, abstraen el requisito de la descentralización abierta. Sirven como un punto de referencia para cuantificar el impacto de este pilar en el rendimiento y la seguridad. La tabla 5.1 aplica el marco de evaluación a esta categoría.

Cuadro 5.1: Comparativa detallada de redes permisionadas.

Criterio	Consorcio	Privada
Eje 1: Escalabilidad		
Rendimiento	Muy Alto (4)	Máximo (5)
Latencia	Rápida (4)	Instantánea (5)
Coste Tx	Bajo (4)	Muy Bajo (5)
Eje 2: Seguridad		
Seg. del modelo	Externa (2)	Externa (1)
Res. antirrobo	Media (3)	Baja (2)
Sup. de confianza	>2/3 Miembros (3)	Operador (1)
Eje 3: Descentralización		
Req. de validación	Controlado (2)	Controlado (1)
Nivel centr.	Gobernanza (2)	Propietario (1)
Res. censura	Baja (2)	Nula (1)

5.3.1. Discusión de la comparativa de redes permisionadas

El análisis de la tabla 5.1 demuestra que las redes blockchain permisionadas representan una elección de diseño arquitectónico deliberada: sacrifican la descentralización y la seguridad criptoeconómica para obtener un sistema de alto rendimiento optimizado para entornos con confianza preexistente.

En el *eje de la escalabilidad*, estas redes alcanzan un rendimiento casi óptimo (4-5) al reemplazar los costosos mecanismos de consenso resistentes a ataque Sybil (como PoW o PoS) por algoritmos de consenso de BFT, como PBFT o sus variantes. Al operar en un entorno no adversario con un conjunto de validadores conocido y limitado, estos protocolos eliminan la necesidad de cómputo intensivo o de un

gran capital en *stake*. Una red *privada (5)* representa el caso límite, funcionando como una base de datos replicada con un único escritor (*leader*), logrando una latencia mínima. Un consorcio (4) introduce una sobrecarga marginal debido a la latencia de comunicación inter-nodos y las rondas de votación necesarias para que el protocolo BFT alcance el consenso entre los miembros.

El *eje de la seguridad* revela un cambio fundamental en el modelo de supuestos. La seguridad no se deriva de incentivos económicos, sino que se fundamenta en un *modelo de confianza basado en la identidad*. La participación está restringida por una lista de control de acceso (ACL) a nivel de red, y la confianza se deposita en la reputación legal y contractual de los operadores. En una red privada, esto se reduce a un único punto de confianza y de fallo (*single point of failure*) en el *operador (1)*. Un consorcio distribuye esta confianza, pero requiere que una supermayoría (típicamente >2/3, un requisito de los protocolos BFT) de los miembros actúe honestamente (3). El riesgo principal aquí no es un ataque externo, sino la *colusión* maliciosa de los miembros del consorcio.

Finalmente, el *eje de la descentralización* es, por diseño, inexistente o mínimo. El término blockchain permisionada se traduce técnicamente en una capa de gestión de identidad, como un MSP, que controla estrictamente los permisos de lectura, escritura y validación. En la red privada, el *propietario (1)* posee privilegios de administrador raíz (*root access*) sobre la topología de la red y el conjunto de validadores. En el consorcio, este control se transfiere a un mecanismo de *gobernanza (2)*, ya sea on-chain o a través de acuerdos legales off-chain, que gestiona la membresía. La resistencia a la censura es baja, ya que el proponente de bloques (*block proposer*), aunque rote, siempre pertenece a un conjunto pequeño y conocido de actores que pueden coordinarse para excluir transacciones.

En conclusión, los datos confirman que las redes blockchain permisionadas no son una variante de las blockchain no permisionadas con menor descentralización, sino una categoría distinta de DLT. Están diseñadas como infraestructuras de coordinación para entidades que ya confían entre sí, priorizando el rendimiento, la finalidad determinista y la gobernanza controlada sobre los principios de apertura y neutralidad de las redes públicas.

5.4. Análisis en Capa 1

Las estrategias de escalado en Capa 1 buscan optimizar el protocolo base. La tabla 5.2 las compara para determinar cuál ofrece el mejor compromiso para fortalecer

la infraestructura fundamental.

Cuadro 5.2: Comparativa detallada de estrategias en Capa 1.

Criterio	+ Límite Gas	PoS	Sharding
Eje 1: Escalabilidad			
Rendimiento	Bajo (2)	Bajo (2)	Alto (4)
Latencia	Lenta (2)	Media (3)	Media (3)
Coste Tx	Alto (2)	Alto (2)	Medio (3)
Eje 2: Seguridad			
Seg. del modelo	Nativo L1 (5)	Nativo L1 (5)	Nativo L1 (5)
Res. antirrobo	Alta (4)	Muy Alta (5)	Muy Alta (5)
Sup. de confianza	>51 % Hashrate (3)	>2/3 Stake (4)	>2/3 Stake (4)
Eje 3: Descentralización			
Req. de validación	Muy Alto (1)	Medio (4)	Bajo (5)
Nivel centr.	Nodos Compl. (2)	Pools Stake (3)	Bajo (4)
Res. censura	Media (3)	Alta (4)	Alta (4)

5.4.1. Discusión de la comparativa en Capa 1

La tabla 5.2 expone los compromisos arquitectónicos en el diseño de protocolos de L1, revelando una clara evolución desde un paradigma monolítico hacia uno modular para resolver el trilema de la blockchain.

En el *eje de la escalabilidad*, el análisis distingue claramente entre soluciones superficiales y mejoras fundamentales. El cuello de botella principal de una blockchain monolítica es su dependencia de una máquina de estado replicada, que procesa transacciones de forma secuencial. Ni el *aumento del límite de gas del bloque* ni el *cambio a PoS* resuelven este problema subyacente, lo que explica sus bajas puntuaciones en *Rendimiento*. En contraste, el sharding es la única estrategia que introduce la paralelización, atacando directamente la raíz del problema y logrando así una mejora sustancial.

En el *eje de la seguridad*, el análisis se centra en cómo cada estrategia de escalado interactúa con el modelo de algoritmo de consenso. La estrategia de *aumento del límite de gas del bloque*, típicamente aplicada sobre una base PoW, hereda su

finalidad probabilística, donde un ataque del 51 % podría teóricamente causar reorganizaciones de la cadena. Por otro lado, tanto la transición a PoS como la implementación de sharding (que generalmente se construye sobre PoS) adoptan un modelo de seguridad criptoeconómico. La innovación clave que ambos comparten es la *finalidad económica*, lograda a través del slashing. Este mecanismo ofrece una garantía determinista contra la reversión de transacciones ya finalizadas. Es esta protección superior contra la "pérdida de fondos" por reversión (un riesgo inherente en los ataques al consenso) lo que justifica la máxima puntuación en *Resistencia antirrobo* para las estrategias basadas en PoS.

Finalmente, en el *eje de la descentralización* se revela el *trade-off* más crítico. El *aumento del límite de gas del bloque* crea un ciclo negativo: al acelerar el crecimiento del estado, incrementa los costes de hardware y expulsa a los operadores pequeños, dañando directamente los *Requisitos de validación* y aumentando el *Nivel de centralización*. El sharding, en cambio, rompe este ciclo. Su innovación clave, el Muestreo de Disponibilidad de Datos (DAS), permite a los nodos verificar la integridad de la red sin descargar todos los datos. Esta reducción drástica de la carga de trabajo es lo que le permite obtener la máxima puntuación en *Requisitos de validación*, democratizando la participación y fortaleciendo la descentralización.

En conclusión, el análisis consolida al *sharding modular* como la arquitectura de L1 más avanzada. Su diseño no solo escala el *Rendimiento*, sino que lo hace reforzando la descentralización, resolviendo así el núcleo del trilema. Esta evolución redefine el rol de la L1: deja de ser una capa de ejecución universal para especializarse en sus competencias nucleares (algoritmo de consenso, disponibilidad de datos y asentamiento), creando la base segura sobre la cual las soluciones de L2 pueden operar como la capa de ejecución de alto rendimiento.

5.5. Análisis en Capa 2 y soluciones híbridas

Esta categoría agrupa a las soluciones que se anclan a una L1 pública, compitiendo por ser la mejor capa de ejecución. La tabla 5.3 es la más crítica para entender el estado actual del escalado.

5.5.1. Discusión de la comparativa Off-Chain

La tabla 5.3 mapea el espectro de soluciones off-chain, revelando los compromisos fundamentales entre escalabilidad, seguridad y descentralización.

Cuadro 5.3: Comparativa detallada de soluciones Off-Chain.

Criterio	Optimistic	ZK-Rollup	Validium	Sidechain
Eje 1: Escalabilidad				
Rendimiento	Alto (4)	Alto (4)	Excelente (5)	Alto (4)
Latencia	Deficiente (1)	Rápida (4)	Rápida (4)	Excelente (5)
Coste Tx	Bajo (4)	Bajo (4)	Muy Bajo (5)	Bajo (4)
Eje 2: Seguridad				
Seg. del modelo	Heredado (5)	Heredado (5)	Híbrido (3)	Propio (2)
Res. antirrobo	Excelente (5)	Excelente (5)	Alta (4)	Baja (2)
Sup. de confianza	Vigilancia 1/N (3)	Criptográfico (5)	DAC honesto (2)	>2/3 Validadores (2)
Eje 3: Descentralización				
Req. de validación	Medio (3)	Alto (2)	Alto (2)	Crítico (1)
Nivel centr.	Sec. (2)	Sec. + Prover (2)	Sec. + DAC (1)	Validadores (2)
Res. censura	Media (3)	Alta (4)	Baja (2)	Baja (2)

En el *eje de la escalabilidad*, todas las soluciones ofrecen un alto *Rendimiento* al externalizar la ejecución. La principal diferencia radica en la gestión de los datos y la finalidad. *Validium* alcanza el *Rendimiento* y *Coste por Transacción* óptimos al mantener los datos fuera de la cadena. Sin embargo, es en la *Latencia* donde se observan las divergencias más críticas: la puntuación deficiente (1) de los *Optimistic Rollups* se debe a su período de disputa de una semana inevitable al hacer uso de la prueba de fraude. En cambio, las soluciones basadas en la prueba de validez (ZK-rollup y *Validium*) y las *sidechains* con su propio algoritmo de consenso ofrecen una finalidad rápida, un requisito indispensable para muchas aplicaciones.

El *eje de la seguridad* es el más revelador y establece una clara jerarquía. Los rollups son los únicos que heredan íntegramente la seguridad de la L1, justificando su máxima puntuación en *Seguridad del modelo* y *Resistencia antirrobo*. Su diseño garantiza que los usuarios puedan recuperar sus activos en la L1 incluso ante un operador malicioso. *Validium* presenta un modelo híbrido: la integridad del estado está asegurada por la prueba de validez, pero la disponibilidad de los datos depende de un DAC, introduciendo un nuevo *Supuesto de confianza* que podría llevar a la congelación de fondos. En el extremo opuesto, la *sidechain* opera con un modelo de seguridad propio y aislado, donde una colusión de sus validadores

puede resultar en la pérdida total de los activos en el puente, lo que explica sus bajas puntuaciones.

Finalmente, en el *eje de la descentralización*, todas las soluciones introducen vectores de centralización significativos en su estado actual. El principal es el rol del secuenciador, un componente que ordena las transacciones y que hoy suele estar operado por una única entidad, lo que explica el bajo valor obtenido, indicando su mala calidad, en el Nivel de centralización. En el caso de los ZK-rollup, se añade la carga computacional del generador de pruebas (*prover*), y en *Validium*, el DAC representa otro punto de centralización. La *Resistencia a la censura* depende de la capacidad de los usuarios para eludir a estos actores centralizados. Los rollups ofrecen las garantías más robustas, ya que los usuarios pueden forzar transacciones directamente en la L1, siendo esta capacidad más directa en los ZK-rollup al no requerir un período de disputa.

5.6. Síntesis del análisis y conclusiones

El análisis cuantitativo de cada categoría converge en una conclusión global: la solución al trilema de la blockchain no reside en una única tecnología monolítica, sino en un cambio de paradigma hacia la *especialización modular*.

La evidencia consolida a la L1 como la capa fundamental de la pila tecnológica, optimizada para ofrecer las máximas garantías de seguridad y descentralización, actuando como la raíz de confianza y la capa de algoritmo de consenso, disponibilidad de datos y asentamiento. Sobre esta base, las soluciones de L2 se establecen como la capa de ejecución de alto rendimiento.

Dentro del ecosistema L2, los rollups emergen como la solución de propósito general por defecto, gracias a su propiedad única de heredar la seguridad de la L1. Entre ellos, los ZK-rollup se perfilan como la tecnología con las propiedades más robustas a largo plazo, al eliminar los supuestos de confianza económicos y los largos períodos de retirada de los *Optimistic Rollups*. Las demás soluciones, como las *sidechains*, los *Validiums* o las redes blockchain permisionadas, no compiten directamente, sino que encuentran su nicho en aplicaciones específicas donde los compromisos de seguridad y descentralización son aceptables a cambio de un rendimiento extremo y costes marginales.

La industria no está convergiendo hacia una «blockchain más rápida», sino hacia una pila tecnológica multicapa. Precisamente, los desafíos abiertos para perfeccionar esta arquitectura, como la descentralización de los secuenciadores en la L2 y la

mejora de la interoperabilidad, constituyen las principales líneas de investigación futuras que se abordarán en el capítulo final.

Capítulo 6

Líneas futuras y desafíos abiertos

El paradigma de la especialización modular, con una L1 como capa de seguridad y las L2s como capa de ejecución, ha consolidado la hoja de ruta para el escalado de blockchain. Sin embargo, esta nueva arquitectura presenta su propio conjunto de desafíos técnicos y áreas de investigación activas que definirán la próxima fase de su evolución.

6.1. Desafíos abiertos en el ecosistema de capa 2

La madurez del ecosistema L2 depende de la resolución de tres problemas fundamentales que afectan directamente a su descentralización, seguridad y usabilidad.

6.1.1. Descentralización del secuenciador y mitigación del MEV

El principal vector de centralización en el ecosistema L2 es el secuenciador. Su control por una única entidad, aunque eficiente, crea un punto de fallo y le otorga un poder casi absoluto sobre la ordenación de transacciones, que es la fuente del Valor Máximo Extraíble (MEV). Al operar un mempool privado, puede reordenar, insertar o censurar transacciones para maximizar su beneficio, lo que impone un "impuesto invisible" a los usuarios a través de ataques como el ataque de anticipación.

La descentralización del secuenciador busca mitigar este poder, pero plantea un desafío fundamental: ¿cómo gestionar el orden de las transacciones de forma jus-

ta y segura sin un único actor de confianza? La investigación ha explorado tres filosofías principales, cada una con su propuesta conceptual original:

1. **Democratización vía subastas.** En lugar de eliminar el MEV, este enfoque busca transformarlo en un mercado transparente. La propuesta seminal fue la *MEV Auction*, que introdujo la idea de subastar el derecho a construir el bloque (Robinson & Konstantopoulos, 2020). Esto separa el rol del secuenciador (que elige al ganador) del constructor (que optimiza el bloque). Así, el MEV pasa de ser un beneficio opaco a un ingreso explícito y redistribuible para la red, resolviendo el monopolio sobre su extracción.

2. **Ocultación de información vía criptografía.** Esta estrategia se basa en un principio simple: un atacante no puede explotar la información que no puede ver. Su origen conceptual se encuentra en protocolos de consenso como *HoneyBadgerBFT*, que fue pionero en integrar el *cifrado de umbral* como parte fundamental del sistema para garantizar la privacidad y la resistencia a la censura (Miller et al., 2016). Al encriptar las transacciones hasta que su orden es definitivo, se ciega a los actores maliciosos y se previenen ataques como el ataque de anticipación.

3. **Neutralización del orden vía consenso justo.** Este es el enfoque más radical, pues busca eliminar la causa raíz del problema: la capacidad misma de reordenar transacciones. Su propuesta fundacional fue la introducción de la equidad de orden (*order-fairness*) como una nueva propiedad de los protocolos de consenso (Kelkar et al., 2020). A través de mecanismos como el propuesto en *Aequitas*, se busca garantizar criptográficamente un orden predecible (ej. FIFO), convirtiendo al secuenciador en un mero ejecutor de reglas y eliminando el poder de reordenación maliciosa.

La elección entre estas arquitecturas (mercado, privacidad o neutralidad) representa uno de los *trade-offs* más importantes en el diseño de las futuras redes de secuenciadores descentralizados, con profundas implicaciones para la seguridad, eficiencia y equidad del ecosistema L2.

6.1.2. Interoperabilidad y fragmentación de la liquidez

El auge de múltiples soluciones de L2 ha creado un ecosistema de "islas" desconectadas. El problema fundamental es que cada rollup tiene su propio secuenciador, que actúa como un director de orquesta independiente. Esto fragmenta la liquidez y fuerza a los usuarios a realizar procesos lentos, costosos y arriesgados a través

de puentes para mover activos entre redes. La falta de un secuenciador común impide la "componibilidad atómica", es decir, la capacidad de realizar una operación compleja que involucre a varias L2s en una única transacción indivisible.

La frontera de la investigación se centra en unificar la secuenciación. La propuesta conceptual de los rollups basados (*based rollups*) aborda este problema de raíz: en lugar de que cada L2 tenga su propio secuenciador, todas heredarían el orden de las transacciones directamente del secuenciador de la L1 (Drake, 2023). Esto crea, en efecto, un "reloj universal" para todo el ecosistema, permitiendo que una transacción en Arbitrum pueda ser ordenada de forma segura y predecible justo antes o después de una en Optimism. El resultado sería una interoperabilidad nativa y segura, donde un usuario podría, por ejemplo, intercambiar un activo en una L2 y depositarlo como colateral en otra, todo ello en una única transacción atómica y sin puentes.

6.1.3. Evolución de arquitecturas híbridas

Las categorías de L2 presentan un dilema rígido. Los rollups ofrecen máxima seguridad al publicar todos los datos en la L1, pero a un coste elevado. Los *Validiums* ofrecen un coste mínimo al mantener los datos fuera de la cadena, pero a cambio de una menor seguridad. Para una aplicación, esta elección es de todo o nada: un juego de alto rendimiento se ve forzado a aceptar una seguridad menor para ser viable económicamente, mientras que un protocolo DeFi que gestiona miles de millones no puede permitirse otra cosa que la máxima seguridad, limitando sus casos de uso.

La próxima frontera es disolver esta dicotomía mediante arquitecturas híbridas. *Volition* articuló esta visión al proponer sistemas que operan en ambos modos simultáneamente (StarkWare, 2021). En lugar de una elección a nivel de protocolo, la flexibilidad se traslada al usuario por cada transacción. Por ejemplo, un inversor podría ejecutar una operación de alto valor y elegir el modo rollup para obtener la seguridad de la L1, pagando una tarifa más alta. Momentos después, podría reclamar una recompensa de bajo valor y elegir el modo *Validium* para esa transacción específica, minimizando el coste. Esta tendencia hacia la modularidad y las arquitecturas "a la carta" sugiere que el futuro no pertenece a una única solución, sino a una gama de sistemas flexibles que se adaptan a las necesidades del usuario en tiempo real.

6.2. La próxima frontera: sinergia con la ciencia de datos e IA

Más allá de las mejoras puramente criptográficas, una línea de investigación emergente, como destaca Rao et al. (Rao et al., 2024), es la aplicación de técnicas de Ciencia de Datos e Inteligencia Artificial. Esto abarca desde el uso de plataformas de análisis de datos en tiempo real para modelar flujos de transacciones y detectar anomalías, hasta la aplicación de *Machine Learning* para optimizar dinámicamente parámetros de la red. Por ejemplo, se podrían desarrollar modelos predictivos para gestionar la congestión de la red, optimizar los mercados de comisiones o incluso mejorar la selección de validadores en sistemas PoS. Esta aproximación interdisciplinar promete abrir una nueva vía de soluciones que complementen los avances en criptografía y sistemas distribuidos.

Capítulo 7

Conclusiones

La conclusión fundamental de este trabajo es que la solución al trilema de la escalabilidad en blockchain no reside en la búsqueda de una única "blockchain más rápida", sino en la adopción de un *paradigma de especialización modular*. Este enfoque, que se ha consolidado como la hoja de ruta de la industria, resuelve la tensión inherente entre descentralización, seguridad y rendimiento de una manera elegante y sostenible.

El análisis ha demostrado que este diseño modular distribuye las responsabilidades de forma óptima: las blockchains de L1 se especializan como capas de asentamiento (*settlement layers*) globales, ofreciendo la máxima seguridad y descentralización, mientras que una vibrante y diversa red de soluciones de L2 se encarga de la ejecución de transacciones a gran escala. En este nuevo paradigma, los rollup emergen como la solución más pragmática y efectiva, al ser los únicos capaces de heredar completamente la seguridad de la L1, combinando así un alto rendimiento con una seguridad robusta.

Esta evolución arquitectónica no es un fenómeno aislado, sino la aplicación directa de principios estudiados a lo largo del Máster. Conceptos de *Computación Paralela* y *Sistemas Distribuidos* explican la eficiencia del *sharding* y la robustez de los algoritmos de consenso en L1, mientras que el modelo de los rollup, que externaliza el cómputo intensivo, refleja las estrategias de escalado y especialización de servicios propias de las *Plataformas de Computación en la Nube*.

Lejos de ser un punto final, este diseño modular define la próxima frontera de investigación y desarrollo. Los desafíos ahora se desplazan hacia la optimización de esta nueva arquitectura, abriendo áreas críticas como la descentralización de los secuenciadores para mitigar el MEV, la creación de protocolos de interoperabili-

dad nativa para unificar la liquidez fragmentada, y la integración con la ciencia de datos para la gestión optimizada de redes.

En definitiva, este trabajo no solo ha cartografiado el complejo panorama de la escalabilidad, sino que ha consolidado una tesis sobre su futuro: uno que es modular, interconectado y que, al resolver el principal cuello de botella de la tecnología, definirá la próxima generación de sistemas blockchain verdaderamente escalables.

Referencias

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 1-15. https://doi.org/10.1145/3190508.3190538 (citado en la p. 26).

Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure* (inf. téc.). Self-published. http://www.hashcash.org/papers/hashcash.pdf (citado en las pp. 2, 15).

Ben DiFrancesco. (2020). Validium and the Layer 2 Two-by-Two [Número 99, consultado el 5 de septiembre de 2025]. https://www.buildblockchain.tech/newsletter/issues/no-99-validium-and-the-layer-2-two-by-two (citado en la p. 40).

Bitcoin Cash. (2017). Bitcoin Cash Specification [Official project documentation]. https://bch.info/en/specifications (citado en la p. 27).

Buterin, V. (2017). The Scalability Trilemma [Blog post]. https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html (citado en las pp. 4, 21).

Buterin, V. (2021). Verkle trees. https://vitalik.eth.limo/general/2021/06/18/verkle.html (citado en la p. 34).

Buterin, V., Feist, D., Loerakker, D., Kadianakis, G., Garnett, M., & Ahmad, M. H. (2022). EIP-4844: Shard Blob Transactions [Ethereum Improvement Proposal]. (Citado en la p. 32).

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99)*, 173-186. https://dl.acm.org/doi/proceedings/10.5555/296806 (citado en la p. 16).

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology: Proceedings of Crypto 82*, 199-203 (citado en la p. 2).

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security*, 106-125. https://doi.org/10.1007/978-3-662-53357-4_8 (citado en las pp. 19, 27, 28).

Dai, W. (1998). b-money. http://www.weidai.com/bmoney.txt (citado en la p. 2).

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. *2020 IEEE Symposium on Security and Privacy (SP)*, 910-927. https://doi.org/10.1109/SP40000.2020.00040 (citado en la p. 20).

Drake, J. (2023). Based rollups—superpowers from L1 sequencing. https://ethresear.ch/t/based-rollups-superpowers-from-l1-sequencing/15016 (citado en la p. 53).

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, *3*(2), 99-111 (citado en la p. 2).

Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, *8*, 125244-125262. https://doi.org/10.1109/ACCESS.2020.3007251 (citado en las pp. 4, 5, 9, 11, 12, 15, 16, 26).

Hardin, G. (1968). The Tragedy of the Commons. *Science*, *162*(3859), 1243-1248 (citado en la p. 20).

Hill, M. D. (1990). What is scalability? *ACM SIGARCH Computer Architecture News*, *18*(4), 18-21. https://doi.org/10.1145/121973.121975 (citado en la p. 17).

Jogalekar, P., & Woodside, M. (2000). Evaluating the scalability of distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, *11*(6), 589-603. https://doi.org/10.1109/71.862209 (citado en las pp. 18, 22).

Kalinin, M., Ryan, D., & Buterin, V. (2021). EIP-3675: Upgrade consensus to Proof-of-Stake [Ethereum Improvement Proposal]. https://eips.ethereum.org/EIPS/eip-3675 (citado en la p. 29).

Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S. M., & Felten, E. W. (2018). Arbitrum: Scalable, private smart contracts. *27th USENIX Security Symposium (USENIX Security 18)*, 1353-1370. https://www.usenix.org/conference/usenixsecurity18/presentation/kalodner (citado en la p. 39).

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. *Cryptology EPrint Archive* (citado en la p. 21).

Kelkar, M., Zhang, F., Goldfeder, S., & Juels, A. (2020). Order-Fairness for Byzantine Consensus. https://eprint.iacr.org/2020/269 (citado en la p. 52).

Lamport, L. (2001). *Paxos Made Simple* (inf. téc. N.º MSR-TR-2001-112). Microsoft Research. https://www.microsoft.com/en-us/research/publication/paxos-made-simple/ (citado en la p. 14).

Lamport, L., Shostak, R. E., & Pease, M. C. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, *4*(3), 382-401. https://doi.org/10.1145/357172.357176 (citado en la p. 14).

Larimer, D. (2017). *EOS.IO Technical White Paper* (White Paper). block.one. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md (citado en la p. 30).

Larimer, D., Hoskinson, C., & Larimer, S. (2014). *BitShares: A Peer-to-Peer Polymorphic Digital Asset Exchange* (White Paper). BitShares. https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf (citado en las pp. 16, 29).

Lombrozo, E., Lau, J., & Wuille, P. (2015). BIP 141: Segregated Witness (Consensus layer) [Bitcoin Improvement Proposal]. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki (citado en la p. 28).

Matter Labs. (2024). zkSync Era Documentation: Introduction [Official project documentation]. https://docs.zksync.io/build/tooling/block-explorer.html (citado en la p. 40).

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The honey badger of BFT protocols. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 31-42 (citado en la p. 52).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (citado en las pp. 1, 10, 12, 14).

Nasir, M. H., Arshad, J., Khan, M. M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains – A systematic review. *Future Generation Computer Systems*, *126*, 136-162. https://doi.org/10.1016/j.future.2021.07.035 (citado en las pp. 3, 5, 11, 13, 15, 26, 29).

Ongaro, D., & Ousterhout, J. (2014). In Search of an Understandable Consensus Algorithm. *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, 305-319. https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro (citado en la p. 14).

Polygon Team. (2024). Polygon PoS Architecture [Official Documentation]. https://docs.polygon.technology/pos/architecture/overview/ (citado en la p. 38).

Poon, J., & Buterin, V. (2017). Plasma: Scalable Autonomous Smart Contracts. https://www.plasma.io/plasma.pdf (citado en la p. 40).

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf (citado en la p. 37).

Popov, S. (2018). *The Tangle* (White paper). IOTA Foundation. https://cryptoverze.s3.us-east-2.amazonaws.com/wp-content/uploads/2018/11/10012054/IOTA-MIOTA-Whitepaper.pdf (citado en la p. 33).

Rao, I. S., Kiah, M. L. M., Hameed, M. M., & Memon, Z. A. (2024). Scalability of blockchain: a comprehensive review and future research direction. *Cluster Computing*, *27*(5), 5547-5570. https://doi.org/10.1007/s10586-023-04257-7 (citado en las pp. 2, 5, 54).

Rebello, G. A. F., Camilo, G. F., de Souza, L. A. C., Potop-Butucaru, M., de Amorim, M. D., Campista, M. E. M., & Costa, L. H. M. K. (2024). A Survey on Blockchain Scalability: From Hardware to Layer-Two Protocols. *IEEE Communications Surveys & Tutorials*, *26*(4), 2411-2458. https://doi.org/10.1109/COMST.2024.3376252 (citado en las pp. 3, 7, 11, 15, 18, 19, 27, 29).

Robinson, D., & Konstantopoulos, G. (2020). MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value. https://ethresear.ch/t/mev-auction-auctioning-transaction-ordering-rights-as-a-solution-to-miner-extractable-value/6788 (citado en la p. 52).

Sanka, A. I., & Cheung, R. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, *195*, 103232. https://doi.org/10.1016/j.jnca.2021.103232 (citado en las pp. 5, 10).

StarkWare. (2021). Volition and the Emerging Data Availability Spectrum. https://starkware.medium.com/volition-and-the-emerging-data-availability-spectrum-87e8bfa09bb (citado en la p. 53).

StarkWare. (2024). StarkEx: How It Works [Official documentation]. https://docs.starkware.co/starkex/overview.html (citado en la p. 40).

Szabo, N. (2005). Bit Gold [Blog post]. https://unenumerated.blogspot.com/2005/12/bit-gold.html (citado en la p. 2).

Visa Inc. (2023). VisaNet Fact Sheet. https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf (citado en la p. 3).

Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger* (Yellow Paper) (Revisión Byzantium. La conceptualización del gas es una parte fundamental de este documento.). Ethereum Project. (Citado en la p. 18).

Yakovenko, A. (2018). *Solana: A new architecture for a high performance blockchain* (inf. téc.). https://solana.com/solana-whitepaper.pdf (citado en la p. 30).

Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., & Liu, R. P. (2020). Survey: Sharding in Blockchains. *IEEE Access*, *8*, 14155-14181. https://doi.org/10.1109/ACCESS.2020.2965147 (citado en la p. 31).

Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., Kiayias, A., & Knottenbelt, W. J. (2019). SoK: Communication Across Distributed Ledgers. https://eprint.iacr.org/2019/1128 (citado en la p. 21).

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, *8*, 16440-16455. https://doi.org/10.1109/ACCESS.2020.2967218 (citado en las pp. 3, 7, 16, 29).

Glosario

algoritmo de consenso Mecanismo que permite a los nodos de una red distribuida ponerse de acuerdo sobre el estado de la misma. Es fundamental para prevenir el problema del doble gasto sin una autoridad central. 2, 10–13, 15, 28, 37, 46–49, 66

ataque de anticipación Estrategia de ataque, común en el contexto del MEV, donde un actor observa una transacción pendiente y utiliza esa información para ejecutar su propia transacción antes, beneficiándose del cambio de precio que la transacción original provocará. En inglés se conoce como *front-running*. 20, 51, 52

ataque del 51 % Ataque potencial a una blockchain, especialmente si usa PoW, donde un atacante controla más del 50 % del poder de la red. Esto le permitiría, por ejemplo, realizar un problema del doble gasto. 15, 22, 27, 47

ataque Sybil Tipo de ataque en un sistema P2P donde un adversario crea múltiples identidades para ganar una influencia desproporcionada. Mecanismos como PoW lo mitigan. 14, 26, 44

blockchain Tipo de DLT que consiste en una cadena de bloques enlazados y asegurados mediante criptografía. Su estructura la hace inherentemente inmutable. i, iii, v, 2, 3, 5, 6, 9–12, 19, 26, 32, 35, 46, 51, 56, 63–67, 69, 70

blockchain no permisionada Red blockchain abierta a cualquiera para participar, sin restricciones de acceso. Prioriza la descentralización. Ej: Bitcoin, Ethereum. 12, 45

blockchain permisionada Red blockchain donde el acceso para participar está restringido a un grupo de entidades autorizadas. 12, 13, 16, 44, 45, 49, 64

calldata Área de datos de solo lectura en una transacción de Ethereum. Es más

barata en términos de gas que el almacenamiento y es clave para el funcionamiento de los rollups de L2. 32

canal de estado Técnica de L2 que permite a los participantes realizar un gran número de transacciones off-chain, registrando únicamente el estado inicial y final en la L1. Requiere que los fondos estén bloqueados y que los participantes monitoricen el canal. 36

consorcio En el contexto de la tecnología blockchain, se refiere a un grupo de organizaciones que colaboran para operar y gobernar conjuntamente una red blockchain permisionada. 16, 26, 45, 71

contrato inteligente Programa autoejecutable que reside en una blockchain y se activa cuando se cumplen condiciones predefinidas, ejecutando acuerdos de forma automática y sin intermediarios. En inglés se conoce como *smart contract*. 10, 11, 18, 19, 66, 69, 70

crecimiento del estado Fenómeno del crecimiento continuo del conjunto de datos que los nodos completos deben mantener para validar nuevas transacciones, amenazando la descentralización. En inglés se conoce como *state bloat*. 19, 20, 22, 27, 34, 47

disponibilidad de datos Garantía de que los datos de las transacciones procesadas por una solución de L2 han sido publicados y están accesibles para que cualquiera pueda verificar el estado. Es una propiedad de seguridad fundamental para los rollups. En inglés se conoce como *data availability*. 36, 38, 47, 49, 69

finalidad Garantía de que una transacción registrada en la blockchain es irreversible y no puede ser alterada. Puede ser probabilística (como en PoW) o determinista (como en algoritmos BFT). 16, 21, 25, 26, 29, 39, 45, 47

gas Unidad que mide el coste computacional de ejecutar operaciones en la EVM. Cada opcode tiene un coste en gas, lo que previene bucles infinitos y compensa a los validadores. 18, 19, 30, 64, 65

hash Función criptográfica que convierte una entrada de cualquier tamaño en una salida de tamaño fijo. Es la base para la integridad de los datos y el encadenamiento de bloques en una blockchain. 9–11, 15, 67

límite de gas del bloque Parámetro en blockchains como Ethereum que define la cantidad máxima de gas que puede ser incluida en un bloque, limitando la cantidad de cómputo por bloque. 19, 22, 27, 30, 46, 47

maleabilidad de las transacciones Fallo de diseño en protocolos como el de Bitcoin (previo a SegWit) que permitía a un tercero alterar el identificador único de una transacción (TXID) antes de que esta fuera confirmada en un bloque. El problema radicaba en que la firma digital, aunque seguía siendo criptográficamente válida tras una sutil modificación, formaba parte de los datos utilizados para generar dicho TXID. Esto creaba incertidumbre y dificultaba el desarrollo de soluciones de segunda capa. Fue solucionado principalmente por la actualización SegWit, que separó los datos de la firma del cálculo del TXID, haciéndolo inmutable. 28, 67

mempool Contracción de *memory pool* (conjunto de memoria). Es el mecanismo que utiliza un nodo de una criptomoneda para almacenar transacciones que han sido enviadas a la red pero que todavía no han sido confirmadas e incluidas en un bloque. Funciona como una sala de espera para las transacciones pendientes. 35, 51

máquina Turing-completa Sistema con un poder computacional equivalente al de una Máquina de Turing universal, capaz de resolver cualquier problema computable. La EVM es un ejemplo. 11, 18

nodo Participante en una red blockchain que mantiene una copia del libro contable y valida transacciones, formando la infraestructura descentralizada de la red. 3, 9–11, 13, 19, 20, 22, 26, 27, 31, 33, 34, 47, 64, 69

off-chain Término que se refiere a transacciones o procesos que se ejecutan fuera de la red principal (L1) de la blockchain, es decir, "fuera de la cadena". 6, 7, 25, 35, 37, 38, 40, 45, 47, 64, 66

on-chain Término que se refiere a todas las transacciones o acciones que ocurren directamente en la red principal (L1) de una blockchain, es decir, "en la cadena". 6, 7, 25, 26, 30, 35, 36, 45

opcode Instrucción de bajo nivel ejecutada por una máquina virtual como la EVM. Es la abreviatura de "código de operación". 18, 30, 64

Paxos Familia de algoritmos de consenso clásicos diseñados para sistemas distribuidos con tolerancia a fallos por caída (CFT), pero no maliciosos. 14, 66,

69

peso de bloque Concepto introducido por SegWit para medir el tamaño de un bloque en la cadena de Bitcoin, reemplazando la limitación estricta de 1 MB por un límite de 4 millones de unidades de peso (WU). Los datos de la transacción pesan 4 WU por byte, mientras que los datos del "testigo" (la firma) pesan solo 1 WU. Este sistema incentiva el uso de transacciones SegWit y permite que quepan más transacciones en un bloque. 28, 67

problema de "nada en juego" Problema teórico en los sistemas PoS donde un validador no tiene ningún perjuicio en apoyar múltiples cadenas, lo que impide el consenso. El slashing es la solución. En inglés se conoce como *nothing-at-stake problem*. 15, 29, 67

problema de los generales bizantinos Problema teórico en computación distribuida que demuestra el desafío de alcanzar un acuerdo en presencia de actores maliciosos. Los algoritmos con BFT lo resuelven. 2, 6, 14, 69

problema del doble gasto Riesgo, en un sistema digital, de que una misma unidad de moneda pueda ser gastada más de una vez. Es el problema fundamental que la blockchain resuelve mediante su algoritmo de consenso. 1, 33, 63

prueba de fraude Mecanismo criptográfico utilizado por los Optimistic Rollups. Permite a cualquier observador demostrar a la L1 que una transición de estado propuesta por un operador de L2 es incorrecta, penalizando al actor malicioso. En inglés se conoce como *fraud proof*. 36, 39, 40, 48

prueba de validez Prueba criptográfica, como un SNARK, utilizada por los ZK-Rollups. Demuestra matemáticamente que un lote de transacciones off-chain ha sido ejecutado correctamente. En inglés se conoce como *validity proof*. 36, 39, 40, 48

puente Protocolo o conjunto de contrato inteligentes que permite la transferencia de activos o datos entre dos blockchains independientes. Son cruciales para la interoperabilidad, pero también son puntos de vulnerabilidad. En inglés se conoce como *bridge*. 21, 35–38, 49, 53

Raft Algoritmo de consenso diseñado como una alternativa a Paxos, con el objetivo de ser más comprensible. También es CFT. 14, 69

rollup Solución de escalado de L2 que procesa transacciones off-chain y luego publica los datos de forma comprimida en la L1, heredando su seguridad.

6, 22, 31, 32, 35, 38, 40, 48, 49, 52, 53, 55, 64, 70

SegWit Actualización del protocolo Bitcoin implementada en 2017 que significa "Testigo Segregado". Solucionó la maleabilidad de las transacciones al separar los datos de la firma (el "testigo") de la parte principal de la transacción. Esta separación también permitió un aumento en la capacidad de transacciones por bloque al introducir una nueva métrica de medida conocida como peso de bloque. 28, 65, 66

sharding Técnica de escalado de L1 que divide la red en fragmentos (*shards*) más pequeños, cada uno capaz de procesar transacciones en paralelo. I, III, V, 6, 22, 31, 32, 46, 47

slashing Mecanismo de castigo en los sistemas PoS donde se le retira una parte de su participación (*stake*) a un validador si actúa de forma deshonesta. Es la principal defensa contra el problema de "nada en juego". 15, 29, 47, 66, 71

trilema de la blockchain Modelo conceptual que postula que las arquitecturas de blockchain se ven forzadas a realizar un compromiso entre tres propiedades: descentralización, seguridad y escalabilidad. 4, 6, 12, 15, 17, 21, 26, 29, 31, 41, 46, 49

verificación universal Propiedad de una blockchain pública que permite a cualquier participante verificar de forma independiente todo el estado y el historial de transacciones de la red. 19, 27

árbol de Merkle Estructura de datos en forma de árbol donde cada nodo hoja es el hash de un bloque de datos, y cada nodo intermedio es el hash de sus hijos. Permiten verificar la inclusión de datos de forma eficiente. 11, 34

Siglas

B2B Modelo de colaboración directa entre empresas (del inglés, *Business-to-Business*). En el ámbito de la DLT, se materializa en redes permisionadas o de consorcio donde la identidad de los participantes es conocida. 13

BFT La capacidad de un sistema para tolerar nodos maliciosos, un concepto clave derivado del problema de los generales bizantinos. Su nombre en inglés es *Byzantine Fault Tolerance*. 13, 14, 26, 44, 45, 64, 66, 71

CFT Modelo de tolerancia a fallos que asume que los nodos pueden dejar de funcionar (caerse), pero nunca actuarán de forma maliciosa. Es el modelo para el que Paxos y Raft fueron diseñados. Su nombre en inglés es *Crash-Fault Tolerance*. 14, 26, 65, 66

DAC Comité de entidades responsables de almacenar los datos de las transacciones en soluciones como los Validiums, introduciendo un nuevo supuesto de confianza. Su nombre en inglés es *Data Availability Committee*. 40, 48, 49

DAG Estructura de datos que generaliza la blockchain. En un DAG, las transacciones se enlazan directamente entre sí, permitiendo un procesamiento paralelo. Es el acrónimo de *Directed Acyclic Graph*. 32

DApp Aplicación digital cuyo backend se ejecuta en una red P2P en lugar de en servidores centrales, a menudo utilizando contrato inteligentes para su lógica. Es el acrónimo de *Decentralized Application*. 11, 29, 30, 39

DAS Técnica que permite a los nodos verificar la disponibilidad de datos de forma eficiente mediante la descarga de pequeñas muestras aleatorias. Su nombre en inglés es *Data Availability Sampling*. 47

DeFi Ecosistema de servicios financieros abiertos basados en tecnología blockchain. Su nombre en inglés es *Decentralized Finance*. 12, 37

DLT Sistema de base de datos distribuida. La blockchain es su implementación más conocida. Su nombre en inglés es *Distributed Ledger Technology*. 9, 26, 45, 63, 69

DPoS Una variante de PoS que utiliza delegados votados para validar bloques y mejorar la eficiencia. Su nombre en inglés es *Delegated Proof-of-Stake*. 16, 29

EIP Documento estándar para proponer cambios al protocolo de Ethereum. Su nombre en inglés es *Ethereum Improvement Proposal*. 29, 31, 32

EVM Entorno de ejecución donde operan los contrato inteligentes en Ethereum. Su nombre en inglés es *Ethereum Virtual Machine*. 10, 18, 30, 39, 64, 65

IA Campo de la informática dedicado a crear sistemas que simulan la inteligencia humana. Su nombre en inglés es *Artificial Intelligence*. 5

IoT Red de dispositivos físicos conectados a internet que recopilan e intercambian datos. Su nombre en inglés es *Internet of Things*. 5

L1 Se refiere a la blockchain base y fundamental de una red. Su nombre en inglés es *Layer 1*. 6, 7, 22, 26, 28, 30–32, 34, 35, 37–40, 46–49, 51, 53, 55, 64–67, 70

L2 Protocolo construido sobre una L1 para mejorar su escalabilidad. Los rollups son un ejemplo. Su nombre en inglés es *Layer 2*. i, iii, v, 6, 7, 21, 22, 27, 28, 31, 32, 35, 36, 38, 40, 47, 49, 51–53, 55, 64, 66

MEV Beneficio que los productores de bloques pueden obtener al reordenar, insertar o censurar transacciones. Es una consecuencia de la transparencia del mempool. Su nombre en inglés es *Maximal Extractable Value*. 20, 35, 51, 52, 55, 63, *véase* mempool

MSP Componente de blockchains permisionadas que gestiona las identidades y permisos de los usuarios. Su nombre en inglés es *Membership Service Provider*. 26, 45

NFT Activo digital único que representa la propiedad de un elemento en una blockchain. Su nombre en inglés es *Non-Fungible Token*. 12

P2P Red descentralizada donde los participantes interactúan directamente sin intermediarios. Su nombre en inglés es *Peer-to-Peer*. 1, 9, 11, 63, 69

PBFT Un algoritmo BFT específico y uno de los primeros en ser lo suficientemente eficiente para ser usado en la práctica, popular en sistemas de consorcio. Su nombre en inglés es *Practical Byzantine Fault Tolerance*. 16, 44

PoS Algoritmo de consenso basado en "apostar" monedas para asegurar la red. Usa slashing como penalización. Su nombre en inglés es *Proof-of-Stake*. 11, 15, 21, 28, 29, 32, 38, 44, 46, 47, 54, 66, 67, 70

PoW Algoritmo de consenso basado en resolver problemas computacionales. Es la base de Bitcoin. Su nombre en inglés es *Proof-of-Work*. 2, 3, 6, 11, 12, 14, 15, 21, 26, 28, 29, 44, 46, 63, 64

SNARK Prueba criptográfica de validez computacionalmente costosa de generar, pero muy eficiente de verificar. Es el pilar de los ZK-Rollups. Su nombre en inglés es *Succinct Non-Interactive Argument of Knowledge*. 36, 39, 66

SO Software fundamental que gestiona el hardware de un ordenador. Su nombre en inglés es *Operating System*. 10

STARK Prueba criptográfica de validez, alternativa a las SNARKs, que se caracteriza por ser *transparente* y *escalable*. La transparencia elimina la necesidad de una 'configuración de confianza', mientras que la escalabilidad la hace eficiente para computaciones de gran tamaño. Generalmente, es resistente a computadoras cuánticas a costa de un mayor tamaño de prueba. Su nombre en inglés es *Scalable Transparent Argument of Knowledge*. 36

TFM Proyecto de investigación requerido para la obtención de un título de máster. i, iii, v, 6

TPS Métrica clave para medir la capacidad y escalabilidad de una red. Su nombre en inglés es *Transactions Per Second*. 3, 4, 16, 18, 26, 27, 29, 42

ZK Campo de la criptografía que permite a una parte (el probador) demostrar a otra (el verificador) que una declaración es cierta, sin revelar información adicional. Su nombre en inglés es *Zero-Knowledge*. 39, 48, 49