

Módulo 3. Tipos de Blockchain y arquitecturas

≡ Tipologías de Blockchain: modelos de acceso y gobernanza

≡ Arquitecturas y criterios de aplicación estratégica

≡ Referencias

Tipologías de Blockchain: modelos de acceso y gobernanza

En el ejercicio profesional vinculado a infraestructuras *blockchain*, una de las decisiones arquitectónicas más relevantes consiste en determinar qué tipo de red resulta adecuada para un caso de uso específico. La elección entre una *blockchain* pública, privada o *permissioned* incide directamente en aspectos como el control del acceso, el modelo de validación, la distribución del poder de decisión y la forma en que se gestiona la información dentro del sistema. En entornos empresariales, gubernamentales o financieros, esta definición condiciona la eficiencia operativa, la trazabilidad, la transparencia y el esquema de responsabilidades entre los actores participantes.

Las redes *blockchain* pueden clasificarse según su nivel de apertura y su estructura de gobernanza. Tal como se describe en la literatura revisada, las redes públicas permiten la participación abierta de cualquier actor, sosteniendo mecanismos de consenso descentralizados y registros inmutables accesibles globalmente. En contraste, las redes privadas restringen la participación a

entidades previamente autorizadas y establecen esquemas de control centralizados o corporativos. Entre ambos extremos se ubican las redes *permissioned* o de consorcio, donde el acceso y la validación se distribuyen entre actores identificados que comparten reglas de operación comunes.

Desde una perspectiva técnica y organizacional, cada tipología implica una configuración particular de nodos validadores, mecanismos de consenso, gestión de identidad y estructura normativa interna. En el ámbito público, la gobernanza se apoya en reglas codificadas y en procesos de consenso abiertos; en los modelos privados y consorciales, las decisiones pueden establecerse mediante acuerdos institucionales o estructuras formales de autoridad.

En esta unidad abordaremos las distintas tipologías de *blockchain* desde el análisis comparativo de sus modelos de acceso y gobernanza. Se examinarán sus características estructurales, sus implicancias operativas y los criterios técnicos que orientan su selección en contextos profesionales concretos, considerando tanto la arquitectura tecnológica como la configuración organizacional que sostiene cada red.

Blockchain pública

La *blockchain* pública constituye un modelo de infraestructura distribuida caracterizado por el acceso abierto, la validación descentralizada y la transparencia del registro. Desde el punto de vista técnico y organizacional, se trata de una red en la que cualquier actor puede participar en la verificación de transacciones, consultar el historial de operaciones y, según el diseño del protocolo, proponer bloques para su incorporación a la cadena. Esta configuración impacta directamente en la forma en que se distribuye el poder de decisión y en cómo se estructura la gobernanza interna del sistema.

En términos conceptuales, una *blockchain* pública **opera como un libro mayor distribuido que mantiene un registro inmutable de transacciones accesible globalmente**. Tal como se expone en la literatura revisada, estos sistemas se apoyan en mecanismos criptográficos y procesos de consenso que permiten validar operaciones sin necesidad de una autoridad central, favoreciendo esquemas de gobernanza descentralizados. Esta arquitectura promueve transparencia, auditabilidad y resistencia frente a manipulaciones unilaterales.

Desde el punto de vista del acceso, las redes públicas permiten que cualquier individuo descargue el software, ejecute un nodo y participe en el proceso de validación. Los materiales analizados

describen este modelo como «*permissionless*», en tanto no requiere autorización previa para interactuar con el sistema. Esta apertura se traduce en una estructura horizontal donde las reglas del protocolo se aplican de manera uniforme a todos los participantes.

En el plano de la validación, los mecanismos de consenso desempeñan un rol operativo central. En redes públicas ampliamente difundidas, los procesos de prueba de trabajo (*proof of work*) o prueba de participación (*proof of stake*) permiten coordinar a miles de nodos distribuidos geográficamente. Según la revisión sistemática presentada en el artículo científico, estos mecanismos aseguran integridad, inmutabilidad y coherencia en entornos donde los actores no necesariamente se conocen entre sí.

La gobernanza en redes públicas se articula a través de reglas codificadas en el protocolo y de dinámicas de participación abierta. Las decisiones sobre actualizaciones, bifurcaciones o modificaciones técnicas suelen surgir de procesos comunitarios donde desarrolladores, validadores y usuarios influyen en la evolución del sistema. En este sentido, la gobernanza combina componentes técnicos —definidos en el código— y dinámicas sociales propias de comunidades distribuidas.

Tabla 1: Características estructurales de la *blockchain* pública

Dimensión	Descripción operativa
Acceso	Abierto a cualquier participante con conexión a internet
Validación	Descentralizada mediante mecanismos de consenso distribuidos
Gestión de identidad	No requiere verificación institucional previa
Registro	Público, transparente e inmutable
Gobernanza	Basada en reglas protocolarias y dinámicas comunitarias

Fuente: elaboración propia.

Desde una perspectiva funcional, la transparencia constituye uno de los atributos más visibles de este modelo. El historial de transacciones puede ser auditado por cualquier actor mediante exploradores de bloques. Esta apertura fortalece la trazabilidad y reduce asimetrías de información en determinados contextos de uso, especialmente cuando se busca maximizar verificabilidad pública.

La inmutabilidad del registro se sustenta en la encadenación criptográfica de bloques y en la replicación del libro mayor entre múltiples nodos. Cualquier intento de alteración requiere modificar simultáneamente una proporción significativa de la red, lo que incrementa los costos operativos de manipulación. Según la literatura revisada, esta propiedad contribuye a reforzar confianza sistémica en entornos descentralizados.

En términos de resistencia a la censura, la ausencia de un controlador central dificulta la exclusión arbitraria de participantes. Dado que la red se sostiene sobre múltiples nodos independientes, la continuidad operativa no depende de una única entidad. Este rasgo resulta especialmente relevante en contextos donde se prioriza autonomía tecnológica y neutralidad infraestructural.

Desde la perspectiva profesional, la *blockchain* pública ofrece **ventajas vinculadas a apertura, interoperabilidad global y robustez frente a intervenciones centralizadas**. Asimismo, facilita la creación de ecosistemas abiertos donde múltiples

desarrolladores pueden construir aplicaciones sobre una misma infraestructura compartida.

Sin embargo, el diseño abierto también introduce limitaciones técnicas y organizacionales. La escalabilidad se ve condicionada por la necesidad de alcanzar consenso entre numerosos nodos distribuidos, lo que puede impactar en la velocidad de procesamiento de transacciones. Además, los costos asociados a determinados mecanismos de consenso —como el consumo energético en algunos esquemas— forman parte de los debates técnicos contemporáneos.

En este sentido, la selección de una *blockchain* pública como infraestructura base requiere evaluar criterios de desempeño, seguridad, gobernanza y modelo de negocio. La arquitectura abierta resulta adecuada cuando se busca maximizar transparencia, neutralidad y participación amplia; en cambio, puede requerir ajustes complementarios cuando las exigencias regulatorias o de confidencialidad demandan mayor control sobre el acceso.

Con ello, la *blockchain* pública se configura como **un modelo arquitectónico orientado a la descentralización plena**, donde la confianza se deposita en reglas protocolarias, mecanismos criptográficos y coordinación distribuida entre actores que operan sin jerarquías centrales.

Mecanismos de consenso en redes públicas

En las redes *blockchain* públicas, los mecanismos de consenso constituyen el procedimiento técnico mediante el cual una comunidad distribuida de nodos acuerda qué transacciones son válidas y en qué orden deben incorporarse al libro mayor. En ausencia de una autoridad central que certifique operaciones, el consenso opera como el dispositivo que garantiza coherencia, integridad y sincronización entre participantes que no necesariamente se conocen entre sí. Desde el punto de vista arquitectónico, el consenso articula criptografía, incentivos económicos y reglas protocolarias.

La literatura revisada sostiene que *blockchain* funciona como un libro mayor distribuido donde la validez de las transacciones se verifica colectivamente a través de algoritmos específicos. En redes públicas, estos algoritmos deben permitir que miles de nodos dispersos geográficamente alcancen acuerdo sin recurrir a confianza previa entre actores. Esta característica define la lógica «permissionless» del sistema, donde cualquier participante puede integrarse al proceso de validación.

Desde una perspectiva técnica, el consenso cumple tres funciones simultáneas: valida transacciones, determina el orden cronológico de los bloques y protege la red frente a intentos de manipulación.

Para ello, se apoya en reglas matemáticas que establecen condiciones objetivas para la aceptación de nuevos bloques. En este sentido, el consenso constituye el núcleo operativo que sostiene la inmutabilidad y la seguridad del registro distribuido.

Principales mecanismos —

En el ámbito de las *blockchain* públicas, dos mecanismos han alcanzado mayor difusión: la prueba de trabajo (*proof of work*, PoW) y la prueba de participación (*proof of stake*, PoS). Ambos responden al mismo objetivo —alcanzar acuerdo descentralizado— aunque difieren en su lógica operativa y en su modelo de incentivos.

La prueba de trabajo se basa en la resolución de problemas criptográficos que requieren capacidad computacional. Los nodos compiten por validar el siguiente bloque realizando cálculos que demandan recursos energéticos. El primero en resolver el desafío obtiene el derecho de proponer el bloque y recibe una recompensa económica. Este mecanismo vincula seguridad con inversión en infraestructura, generando una barrera técnica frente a ataques coordinados.

En contraste, la prueba de participación asigna el derecho de validación en función de la cantidad de activos que un nodo mantiene en depósito dentro del sistema. El consenso se apoya en la participación económica comprometida, reduciendo el requerimiento de poder computacional intensivo. Este modelo introduce un diseño diferente de incentivos, donde la seguridad se relaciona con la exposición financiera del validador dentro del ecosistema.

Tabla 2. Comparación técnica entre PoW y PoS

Criterio	Prueba de trabajo (PoW)	Prueba de participación (PoS)
-----------------	--------------------------------	--------------------------------------

Recurso principal	Potencia computacional	Activos en depósito.
Incentivo	Recompensa por bloque minado	Recompensa por validación proporcional al <i>stake</i> .
Consumo energético	Elevado	Reducido en comparación.
Seguridad	Basada en costo computacional del ataque	Basada en costo económico del ataque.
Participación	Abierta a quienes dispongan de hardware adecuado	Abierta a quienes mantengan participación económica.

Fuente: elaboración propia.

Ambos mecanismos buscan resolver el problema del «doble gasto» en entornos descentralizados, asegurando que una misma unidad de valor no pueda utilizarse más de una vez. Este desafío resulta especialmente relevante en sistemas donde no existe una entidad central que supervise las transacciones. El consenso establece reglas verificables que impiden inconsistencias contables.

Desde la perspectiva de gobernanza, los mecanismos de consenso también influyen en la distribución del poder dentro de la red. En PoW, los actores con mayor capacidad computacional tienden a concentrar capacidad de validación; en PoS, la influencia se relaciona con la proporción de activos comprometidos. En ambos casos, la arquitectura técnica modela dinámicas organizacionales internas y condiciona la evolución del sistema.

Esquema conceptual

—

Funcionamiento general del consenso en redes públicas

1. Un usuario emite una transacción.
2. La transacción se difunde a los nodos de la red.
3. Los nodos validan la coherencia criptográfica de la operación.
4. Los validadores compiten o son seleccionados según el algoritmo de consenso.
5. Se propone un bloque con transacciones verificadas.
6. La red alcanza acuerdo y replica el bloque en todos los nodos.

Este proceso permite mantener sincronizado el libro mayor distribuido sin necesidad de intermediarios. La coordinación se sostiene en reglas automáticas ejecutadas por el protocolo, lo que refuerza la transparencia y la auditabilidad del sistema.

En términos profesionales, comprender los mecanismos de consenso resulta determinante al momento de diseñar soluciones sobre redes públicas. La elección del algoritmo impacta en el rendimiento, la seguridad, los costos operativos y el modelo de incentivos económicos del ecosistema. Por ello, el consenso constituye un componente estructural de la arquitectura *blockchain* y un eje central en la evaluación técnica de cualquier infraestructura pública.

Ventajas y limitaciones de la *blockchain* pública

Las redes *blockchain* públicas se caracterizan por su **acceso abierto** y su **validación descentralizada**. Este diseño produce efectos técnicos y organizacionales específicos que deben analizarse en términos de ventajas y limitaciones operativas. Desde una perspectiva de infraestructura, la arquitectura abierta favorece transparencia y auditabilidad, aunque también introduce

desafíos vinculados al rendimiento y a la coordinación entre actores distribuidos.

En relación con la **escalabilidad**, el consenso distribuido entre numerosos nodos garantiza seguridad e integridad, pero puede impactar en la velocidad de procesamiento de transacciones. La necesidad de alcanzar acuerdo colectivo implica tiempos de confirmación más extensos en comparación con sistemas centralizados. Este rasgo forma parte del equilibrio técnico entre descentralización y eficiencia operativa.

En cuanto a los **costos**, los mecanismos de consenso utilizados en redes públicas pueden implicar gastos significativos, ya sea por consumo energético en modelos basados en prueba de trabajo o por requerimientos económicos en esquemas de participación. Estos costos forman parte del diseño de incentivos que sostiene la seguridad de la red.

Respecto de la **gobernanza abierta**, la toma de decisiones se apoya en reglas protocolarias y dinámicas comunitarias. Las actualizaciones y modificaciones requieren coordinación entre desarrolladores, validadores y usuarios, lo que promueve transparencia, pero también puede generar procesos deliberativos extensos.

Tabla 3. **Ventajas y limitaciones de la *blockchain* pública**

Dimensión	Ventajas	Limitaciones
Escalabilidad	Alta seguridad y robustez frente a manipulaciones	Procesamiento más lento por consenso distribuido
Costos	Incentivos alineados con seguridad de la red	Costos energéticos o económicos asociados al consenso
Gobernanza abierta	Transparencia y participación amplia	Coordinación compleja para implementar cambios

Fuente: elaboración propia.

En síntesis, la blockchain pública ofrece un modelo de infraestructura orientado a maximizar descentralización y transparencia. Al mismo tiempo, su diseño requiere gestionar cuidadosamente el equilibrio entre seguridad, eficiencia y procesos de decisión colectiva.

Blockchain privada y permissioned

Las redes *blockchain* privadas y *permissioned* surgen como variantes arquitectónicas orientadas a contextos organizacionales donde la gestión del acceso, la identidad de los participantes y el control operativo requieren mayor estructuración institucional. A diferencia de las redes públicas abiertas, estos modelos restringen la participación a actores previamente autorizados, configurando entornos donde la gobernanza se articula mediante reglas formales y acuerdos entre entidades identificables.

De acuerdo con Seth (2018), las *blockchains* privadas se caracterizan por operar bajo el control de una organización específica que determina quién puede leer, escribir o validar transacciones dentro de la red. Este diseño introduce una estructura jerárquica clara en la gestión del sistema, permitiendo establecer políticas internas de seguridad, confidencialidad y cumplimiento normativo.

En la misma línea, CoinGeek (s. f.) distingue entre *blockchain* privada y *blockchain permissioned*, señalando que ambas comparten restricciones de acceso, aunque difieren en la forma en que se distribuye el control. Mientras la red privada suele estar

gobernada por una única entidad, la red *permissioned* puede estructurarse como un consorcio donde múltiples organizaciones comparten responsabilidades de validación bajo reglas previamente acordadas.

Abanca Innova (s. f.) explica que este modelo resulta particularmente adecuado en entornos empresariales o financieros donde se requiere trazabilidad compartida sin exponer información sensible al público general. En estos casos, la red mantiene las propiedades técnicas de integridad y encadenamiento criptográfico, aunque limita la visibilidad y participación externa.

Diferencias entre red privada y red *permissioned*

En una *blockchain* privada, la autoridad que administra la red define el esquema de nodos validadores y controla las reglas de incorporación de nuevos participantes. El consenso puede alcanzarse mediante algoritmos menos costosos que los utilizados en redes públicas, dado que los actores están identificados y operan bajo marcos contractuales definidos (Seth, 2018).

Por su parte, la *blockchain permissioned* distribuye la validación entre entidades previamente autorizadas, lo que configura un

modelo de gobernanza consorcial. Según CFTE (s. f.), este esquema permite combinar eficiencia operativa con descentralización parcial, dado que ningún actor individual concentra completamente el control, aunque el acceso permanece regulado.

Tabla 4. Comparación estructural: *blockchain* privada vs. *permissioned*

Dimensión	<i>Blockchain</i> privada	<i>Blockchain</i> permissioned
Control	Centralizado en una organización	Distribuido entre entidades autorizadas.
Acceso	Restringido por administrador	Restringido por reglas del consorcio.
Validación	Nodos designados por la entidad controladora	Nodos validados por acuerdo institucional.

Transparencia	Limitada al entorno interno	Compartida entre miembros autorizados.
Caso de uso frecuente	Gestión interna empresarial	Redes interinstitucionales.

Fuente: elaboración propia con base en Seth (2018).

Control de acceso y validadores autorizados

El control de acceso constituye uno de los rasgos distintivos de estos modelos. Los participantes deben cumplir requisitos de identidad y autorización antes de interactuar con la red. Este diseño reduce la incertidumbre respecto de quién valida las transacciones y permite implementar políticas de cumplimiento regulatorio más estrictas (Abanca Innova, s. f.).

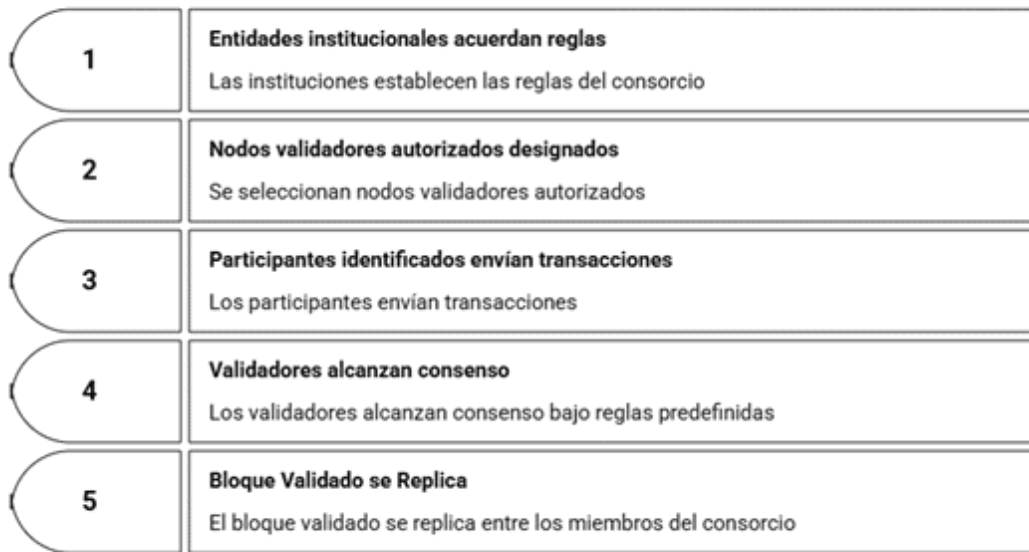
En términos de consenso, al operar con un número limitado de nodos identificados, estas redes pueden emplear mecanismos más ágiles que los utilizados en entornos públicos. La eficiencia operativa se incrementa al disminuir la necesidad de coordinación masiva entre participantes anónimos (CoinGeek, s. f.).

Gobernanza cerrada vs. gobernanza consorcial

La gobernanza en redes privadas se estructura mediante decisiones internas de la organización administradora. Las actualizaciones del protocolo, la incorporación de nodos y las reglas de validación se definen de manera centralizada.

En cambio, la gobernanza consorcial se basa en acuerdos entre múltiples instituciones. Según Ibrahimy, Norta y Normak (2023), los modelos de gobernanza *blockchain* pueden configurarse para equilibrar transparencia, control y cooperación interorganizacional, especialmente en contextos donde la coordinación entre actores requiere reglas claras y trazabilidad compartida.

Figura 1. Modelo operativo de una *blockchain permissioned*



Made with  Napkin

Fuente: elaboración propia.

Este modelo combina elementos de descentralización técnica con control organizacional, permitiendo eficiencia y confidencialidad en entornos regulados.

Seguridad, eficiencia y trazabilidad empresarial

Desde la perspectiva profesional, las redes privadas y *permissioned* resultan adecuadas cuando se requiere:

- Protección de datos sensibles.
- Cumplimiento normativo sectorial.

- Alta velocidad de procesamiento.
- Coordinación entre instituciones con responsabilidades definidas.

Seth (2018) destaca que estos modelos sacrifican apertura total en favor de control y rendimiento. Por su parte, Abanca Innova (s. f.) señala que su adopción se vincula con sectores como banca, logística y administración pública, donde la trazabilidad compartida aporta valor sin requerir exposición pública del registro.

En síntesis, las *blockchain* privadas y *permissioned* representan arquitecturas orientadas a la eficiencia operativa y a la gobernanza institucional. Su diseño responde a necesidades organizacionales específicas, priorizando control de acceso, validación autorizada y cumplimiento normativo sobre la apertura universal característica de las redes públicas.

Para cerrar el desarrollo, resulta pertinente integrar comparativamente los tres modelos analizados: *blockchain* pública, privada y *permissioned*. A lo largo del desarrollo se examinó cómo cada arquitectura configura de manera diferente el acceso a la red, el mecanismo de validación y la

estructura de gobernanza. Sin embargo, desde el ejercicio profesional, la toma de decisiones tecnológicas requiere una visión sintética que permita contrastar estos modelos bajo criterios comunes.

Como señalan Seth (2018), la distinción entre redes abiertas y redes con permisos no responde únicamente a una diferencia técnica, sino también organizacional y estratégica. Del mismo modo, Abanca Innova (s. f.) subraya que la elección del tipo de *blockchain* depende del grado de transparencia requerido, del nivel de control institucional y de las exigencias regulatorias del entorno donde se implementa la solución. En esta línea, Ibrahimy, Norta y Normak (2023) destacan que los modelos de gobernanza influyen directamente en la forma en que se distribuyen responsabilidades, poder de decisión y mecanismos de supervisión dentro del ecosistema.

En consecuencia, la siguiente tabla resume las principales diferencias estructurales entre los tres tipos de redes, permitiendo visualizar de manera integrada los criterios técnicos y organizacionales trabajados en la unidad.

Tabla 5. Comparación general entre *blockchain* pública, privada y *permissioned*

Dimensión	<i>Blockchain pública</i>	<i>Blockchain privada</i>	<i>Blockchain permissioned</i>
Acceso	Abierto a cualquier participante (Seth, 2018)	Restringido por una entidad central	Restringido a miembros autorizados (CoinGeek, s. f.)
Validación	Descentralizada y abierta	Controlada por la organización	Distribuida entre validadores designados
Gobernanza	Comunitaria y basada en protocolo (Ibrahimi et al., 2023)	Jerárquica o corporativa	ConSORcial o interinstitucional
Transparencia	Registro público y auditable	Limitada al entorno interno	Compartida entre miembros
Escalabilidad	Condicionada por consenso	Mayor eficiencia	Equilibrio entre control y

	masivo		operativa	rendimiento
Casos de uso frecuentes	Criptoactivos, redes abiertas		Gestión interna empresarial	Redes financieras, logísticas o sectoriales

Fuente: elaboración propia con base en Seth (2018).

Esta comparación permite comprender que las tipologías de *blockchain* no representan grados de avance tecnológico, sino configuraciones diferenciadas orientadas a resolver necesidades específicas. Mientras la red pública prioriza apertura y descentralización, los modelos privados y *permissioned* enfatizan control institucional, eficiencia y cumplimiento normativo.

CONTINUAR

Arquitecturas y criterios de aplicación estratégica

En el ejercicio profesional vinculado al diseño de infraestructuras *blockchain*, la definición del tipo de red constituye solo una primera decisión. Una vez seleccionado el modelo de acceso y gobernanza, el desafío se traslada al plano arquitectónico: cómo estructurar los nodos, cómo organizar las capas funcionales, qué mecanismos de validación implementar y cómo garantizar interoperabilidad y escalabilidad según el caso de uso. En esta etapa, las decisiones técnicas adquieren un carácter estratégico, ya que impactan directamente en la viabilidad operativa, el rendimiento y la sostenibilidad del sistema en el tiempo.

Las investigaciones recientes sobre arquitectura de red señalan que el rendimiento de una *blockchain* no depende únicamente del algoritmo de consenso, sino también de su topología, de los mecanismos de comunicación entre nodos y de la organización de sus capas funcionales. Zhou, Han y Li (2025), en su propuesta de arquitectura basada en *information-centric networking*, muestran que la optimización de la comunicación entre nodos puede

reducir latencias y mejorar la eficiencia del *broadcast* en redes de gran escala. Este enfoque evidencia que la arquitectura de red constituye un componente determinante para la performance global del sistema.

Asimismo, la implementación práctica de nodos validadores demuestra que la arquitectura no se limita al diseño lógico, sino que involucra decisiones concretas sobre infraestructura, clientes de software, capas de ejecución y capas de consenso. En el caso de Ethereum, por ejemplo, el funcionamiento del nodo validador articula componentes diferenciados que participan en la propuesta y validación de bloques bajo esquemas de prueba de participación (Launchnodes, 2024).

En esta unidad abordaremos los criterios técnicos que orientan el diseño de arquitecturas *blockchain* y analizaremos cómo dichas configuraciones se vinculan con casos de uso específicos. Se examinarán los componentes estructurales de la red, los modelos híbridos, la interoperabilidad y los desafíos de escalabilidad, para luego relacionarlos con aplicaciones concretas en finanzas descentralizadas, trazabilidad, identidad digital y entornos gubernamentales.

Arquitectura *blockchain* y diseño de red

El diseño de una arquitectura *blockchain* implica definir cómo se organizan sus componentes estructurales, cómo interactúan los nodos y qué mecanismos garantizan coherencia, rendimiento y seguridad en la red. Desde una perspectiva técnica, la arquitectura determina la topología de comunicación, la forma en que se transmiten bloques y transacciones, y la manera en que se optimiza el uso del ancho de banda. Desde una perspectiva operativa, implica decidir qué tipo de nodos se implementan, cómo se configuran los validadores y cómo se articulan las capas funcionales del sistema.

Zhou, Han y Li (2025) sostienen que el rendimiento de una red *blockchain* depende en gran medida de su arquitectura de comunicación. En su propuesta basada en *information-centric networking*, demuestran que la organización jerárquica de nodos y la optimización del *broadcast* pueden reducir latencias y consumo de ancho de banda en redes de gran escala. Este enfoque técnico evidencia que la eficiencia no depende exclusivamente del consenso, sino también de la estructura de red y de los mecanismos de propagación de información.

En paralelo, el análisis operativo de nodos validadores en Ethereum muestra que la arquitectura se materializa en decisiones concretas de infraestructura. Launchnodes (2024) explica que un nodo validador articula al menos dos capas diferenciadas: la capa de ejecución y la capa de consenso. Esta

separación funcional impacta directamente en el diseño del sistema, ya que cada capa cumple responsabilidades específicas dentro del proceso de validación.

Componentes estructurales de una red blockchain

Una arquitectura *blockchain* puede descomponerse en los siguientes componentes:

- **Nodos completos:** almacenan la totalidad del libro mayor y validan transacciones.
- **Nodos validadores:** participan activamente en el consenso y en la propuesta o atestiguación de bloques.
- **Clientes de ejecución:** gestionan el estado, ejecutan contratos inteligentes y mantienen la lógica de negocio.
- **Clientes de consenso:** coordinan el mecanismo de validación y sincronizan la red.
- **Capa de red:** define la topología P2P y los protocolos de comunicación.
- **Capa de aplicación:** aloja contratos inteligentes y servicios descentralizados.

Zhou et al. (2025) enfatizan que la capa de red y la topología influyen directamente en la latencia de propagación de bloques. Una estructura optimizada reduce redundancias en la transmisión de datos y mejora la escalabilidad. Por su parte, Launchnodes (2024) muestra que, desde el plano operativo, la correcta configuración de clientes y validadores resulta determinante para garantizar estabilidad y rendimiento.

Tabla 6. Capas funcionales y responsabilidades en una arquitectura *blockchain*

Capa	Función técnica	Función operativa
Red	Propagación de bloques y transacciones	Configuración de conectividad P2P
Consenso	Validación y ordenamiento de bloques	Operación de nodos validadores

Ejecución	Gestión del estado y contratos inteligentes	Instalación y mantenimiento de clientes
Aplicación	Servicios y lógica de negocio	Desarrollo e implementación de soluciones

Fuente: elaboración propia con base en Zhou et al. (2025).

Modelos híbridos

Las arquitecturas híbridas combinan elementos de redes públicas y privadas o integran infraestructuras externas para optimizar rendimiento. Zhou et al. (2025) proponen una arquitectura compatible con entornos IP e ICN, permitiendo mejorar eficiencia sin alterar completamente la infraestructura existente. Este tipo de diseño facilita transiciones progresivas y reduce fricciones técnicas.

En términos operativos, los modelos híbridos pueden incluir:

- Validadores distribuidos en nube pública.
- Nodos internos para procesamiento sensible.
- Puentes (*bridges*) para interoperabilidad entre redes.

Interoperabilidad entre redes

La interoperabilidad constituye un criterio estratégico en arquitecturas modernas. Permite que distintas redes *blockchain* intercambien información o activos. Desde el plano técnico, implica **protocolos de comunicación estandarizados** y **mecanismos de verificación cruzada**. Desde el plano operativo, requiere **herramientas de orquestación y monitoreo que garanticen coherencia entre sistemas heterogéneos**.

Escalabilidad y performance

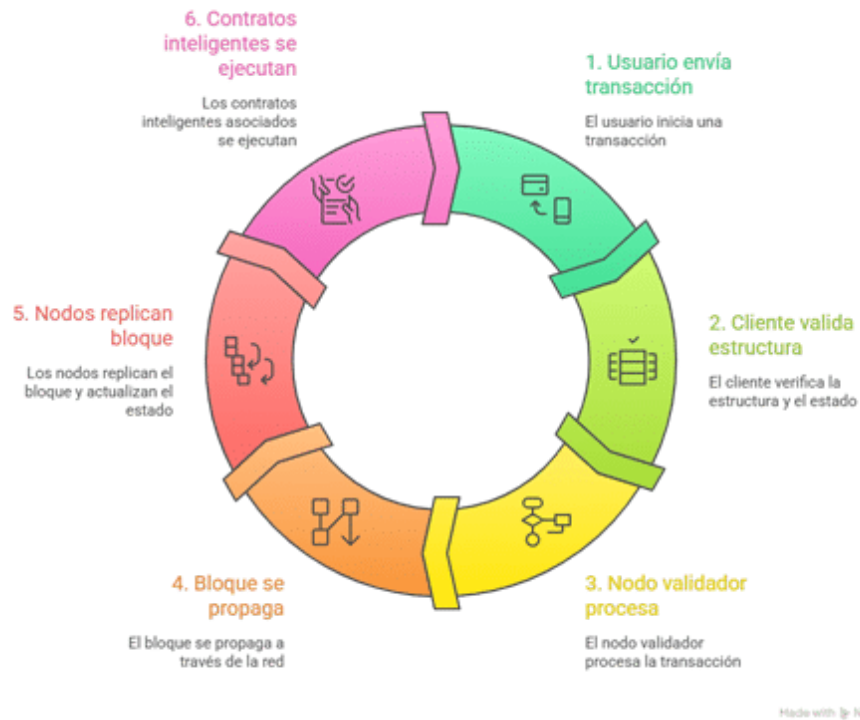
Zhou et al. (2025) demuestran que la optimización del *broadcast* y la partición de dominios puede reducir la latencia en escenarios con miles de nodos. Esto evidencia que la performance depende tanto del consenso como de la arquitectura de red. La reducción de redundancias y la mejora en la topología permiten aumentar cobertura sin comprometer estabilidad.

Operativamente, la escalabilidad también depende de:

- Capacidad de hardware del nodo.
- Distribución geográfica de validadores.
- Configuración de clientes de ejecución y consenso.

- Gestión eficiente del ancho de banda.

Figura 2. Arquitectura integrada de red *blockchain*



Fuente: elaboración propia.

Esta imagen muestra cómo interactúan las capas técnicas y las decisiones operativas dentro de una arquitectura coherente.



Entonces, el diseño arquitectónico blockchain exige integrar criterios técnicos —topología, broadcast, latencia— con decisiones operativas —infraestructura, validadores, clientes y monitoreo—. La articulación equilibrada de ambos enfoques permite construir redes escalables, interoperables y alineadas con los objetivos estratégicos del caso de uso.

Casos de uso según arquitectura

La arquitectura *blockchain* adquiere sentido estratégico cuando se la vincula con escenarios de aplicación concretos. Las decisiones técnicas relativas a capas funcionales, nodos validadores, topología de red e interoperabilidad no se adoptan en abstracto, sino en función de objetivos operativos específicos. En este marco, la relación entre arquitectura y caso de uso determina el equilibrio entre descentralización, rendimiento, confidencialidad y cumplimiento normativo.

Zhou, Han y Li (2025) muestran que la optimización de la arquitectura de red incide directamente en la eficiencia del sistema, aspecto particularmente relevante en aplicaciones que requieren alta frecuencia transaccional. Por su parte, Launchnodes (2024) evidencia que la correcta configuración de

nodos validadores resulta determinante en redes que operan bajo esquemas de prueba de participación, donde la estabilidad y disponibilidad del nodo influyen en la seguridad y en la obtención de recompensas.

A continuación, se analizan distintos casos de uso y su correspondencia arquitectónica.

Finanzas descentralizadas (DeFi) —

Las aplicaciones DeFi requieren:

- Alta disponibilidad de nodos.
- Validación continua y segura.
- Ejecución eficiente de contratos inteligentes.
- Interoperabilidad con múltiples protocolos.

En este entorno, la arquitectura prioriza:

- Separación clara entre capa de ejecución y capa de consenso.
- Nodos validadores distribuidos geográficamente.
- Infraestructura robusta con monitoreo constante.

La eficiencia en la propagación de bloques, tal como señalan Zhou et al. (2025), resulta central para reducir latencias en operaciones financieras automatizadas. La dimensión operativa, destacada por Launchnodes (2024), se manifiesta en la necesidad de mantener nodos actualizados y correctamente configurados para evitar penalizaciones o interrupciones.

Trazabilidad y supply chain —

En cadenas de suministro, la arquitectura suele orientarse hacia:

- Redes *permissioned* o híbridas.
- Validadores institucionales identificados.
- Integración con sistemas empresariales existentes.

La interoperabilidad permite conectar sistemas logísticos con *blockchain*, asegurando trazabilidad compartida. En estos casos, la performance depende más de la estabilidad y de la integridad de datos que de la descentralización absoluta.

Identidad digital —

Los sistemas de identidad digital demandan:

- Seguridad criptográfica robusta.
- Protección de datos personales.
- Arquitectura que permita validación selectiva.

En este contexto, pueden emplearse modelos híbridos donde la capa pública garantiza inmutabilidad, mientras que capas privadas gestionan información sensible. La arquitectura debe equilibrar transparencia y confidencialidad.

Tokenización de activos —

La *tokenización* implica representar activos físicos o financieros en una *blockchain*. Arquitectónicamente requiere:

- Capa de ejecución eficiente para contratos inteligentes.
- Interoperabilidad entre redes.
- Capacidad de escalado para gestionar múltiples emisiones.

La topología de red influye en la velocidad de confirmación, aspecto relevante cuando se integran mercados secundarios o plataformas de intercambio.

Aplicaciones gubernamentales y corporativas —

En entornos gubernamentales o corporativos, la arquitectura prioriza:

- Gobernanza clara y validadores autorizados.
- Cumplimiento normativo.
- Registro auditable pero con acceso controlado.

Los modelos *permissioned* o consorciales permiten distribuir responsabilidades sin perder control institucional. La arquitectura técnica debe integrarse con infraestructuras existentes y garantizar estabilidad a largo plazo.

La siguiente tabla sintetiza la relación entre tipo de aplicación y criterio arquitectónico predominante, permitiendo visualizar cómo las decisiones técnicas y operativas se ajustan a los objetivos estratégicos de cada caso de uso. En lugar de asumir una arquitectura uniforme

para todas las implementaciones, el cuadro muestra que la elección depende del equilibrio requerido entre rendimiento, control institucional, interoperabilidad y nivel de descentralización. De este modo, la arquitectura se comprende como una variable estratégica que se configura en función de las necesidades específicas del entorno donde se despliega la solución *blockchain*.

Tabla 7. Correspondencia entre caso de uso y criterio arquitectónico

Caso de uso	Tipo de arquitectura frecuente	Prioridad técnica	Prioridad operativa
DeFi	Pública	Baja latencia y alto <i>throughput</i>	Alta disponibilidad de validadores
<i>Supply chain</i>	<i>Permissioned</i> / híbrida	Integridad y trazabilidad	Integración con sistemas empresariales
Identidad digital	Híbrida	Seguridad criptográfica	Protección de datos sensibles

<i>Tokenización</i>	Pública o híbrida	Escalabilidad	Interoperabilidad entre plataformas
Gobierno / corporativo	<i>Permissioned</i>	Estabilidad y control	Cumplimiento normativo

Fuente: elaboración propia.

En conclusión, la arquitectura blockchain no constituye un diseño único aplicable universalmente. Cada caso de uso demanda una combinación específica de topología de red, configuración de nodos, modelo de consenso y esquema de gobernanza. La decisión estratégica radica en identificar qué dimensión —descentralización, rendimiento, confidencialidad o interoperabilidad— resulta prioritaria en cada contexto.

CONTINUAR

Referencias

Abanca Innova. (s. f.). *Los tipos de blockchain pública, privada o consorcio explicados.* Abanca Innova. <https://abancainnova.com/los-tipos-de-blockchain-publica-privada-o-consorcio-explicados/>

CFTE. (s. f.). *What is public blockchain?* CFTE Blog. <https://blog.cfte.education/what-is-public-blockchain/>

CoinGeek Media. (s. f.). *Private vs. public vs. permissioned blockchain: A comparative guide.* CoinGeek. <https://coingeek.com/blockchain101/private-vs-public-vs-permissioned-blockchain-a-comparative-guide/>

Ibrahimy, M., Norta, A., & Normak, P. (2023). *Blockchain-based governance models supporting corruption-transparency: A systematic literature review.* *Blockchain: Research and Applications*, 5(2), 100186. <https://doi.org/10.1016/j.bcra.2023.100186>

Launchnodes. (2024). *What is a validator node and how do you run one as a solo staker?* <https://www.launchnodes.com/what-is-a-validator-node-and-how-do-you-run-one-as-a-solo-staker/>

Seth, S. (2018, 10 de abril). *Public, private, and permissioned blockchains compared.* Investopedia. <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>

Zhou, X., Han, Y., & Li, Z. (2025). A blockchain network communication architecture based on information-centric networking. *Applied Sciences*, 15(6), 3340. <https://doi.org/10.3390/app15063340>

CONTINUAR