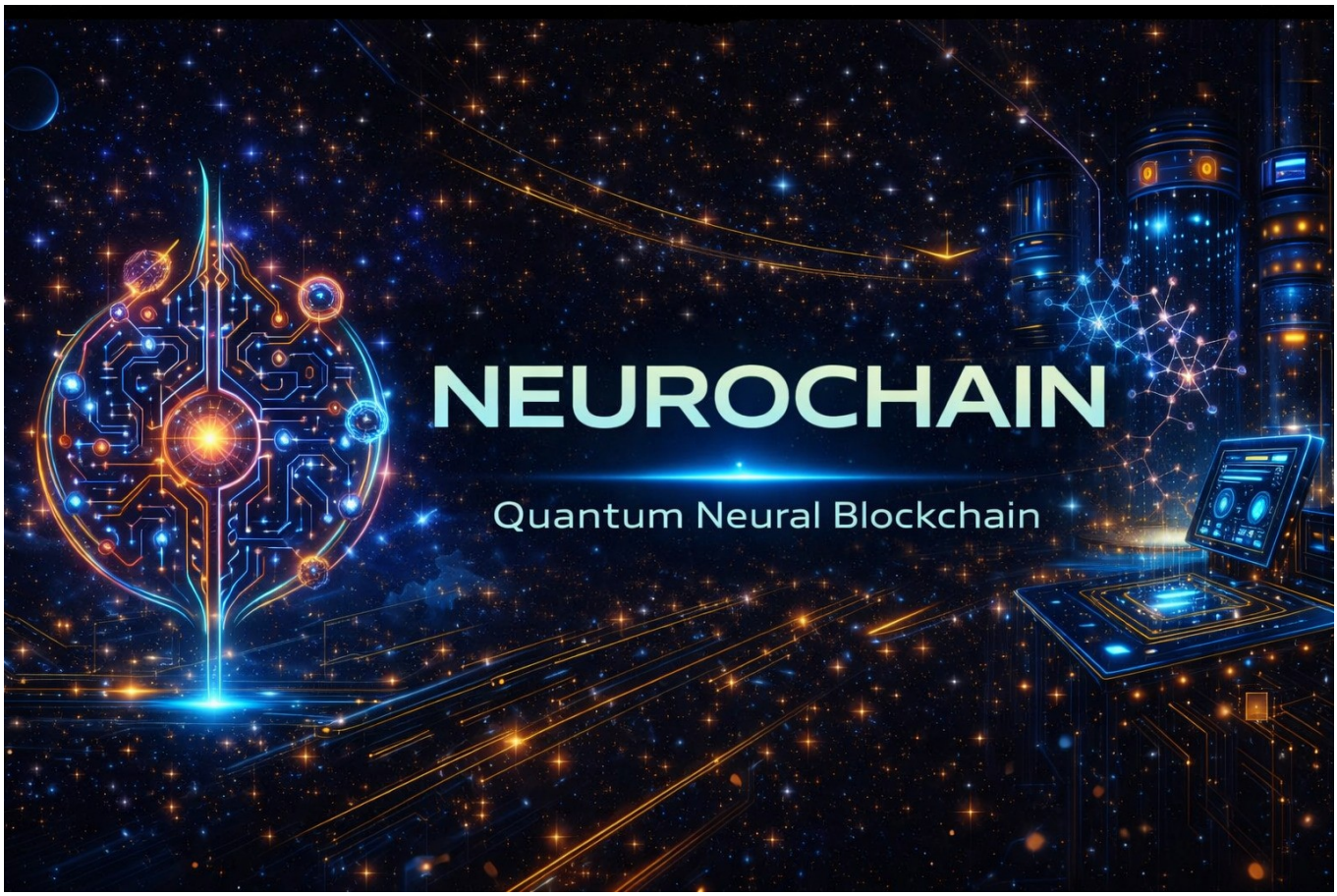

STRATEGIC & TECHNICAL ARCHITECTURE DOSSIER

Expository + Technical Overview • Non-Implementation Disclosure

Version 0.1 | August 2026 | Confidential

"Una L1 cognitiva, post-cuántica, financiera, escalable y evolutiva."

00

Control del documento y alcance

Documento conceptual de arquitectura; no contiene secretos operativos, claves, parámetros finales ni código de producción.

Este dossier consolida la visión discutida para NEUROCHAIN desde su concepción como una Layer 1 con inteligencia artificial nativa y seguridad post-cuántica, hasta la definición de un modelo de consenso, una capa financiera ISO 20022, un mecanismo de resiliencia evolutiva, interoperabilidad con wallets existentes y una ruta de rendimiento orientada a 200.000 transacciones finalizadas de forma segura por segundo (SFTPS).

Límite de divulgación — El documento explica el qué, el por qué y el cómo a nivel arquitectónico. Deliberadamente no publica detalles internos que podrían convertirse en superficie de ataque: lógica exacta de selección de committees, formatos definitivos de mensajes de consenso, umbrales internos, derivación de claves, políticas de slashing finales, mecanismos antifraude específicos, reglas de actualización de emergencia ni configuraciones de infraestructura productiva.

Campo	Definición
Nombre	NEUROCHAIN — Strategic & Technical Architecture Dossier
Marca técnica	Quantum Neural Blockchain
Versión	0.1 conceptual
Clasificación	Confidencial / arquitectura de alto nivel
Objetivo	Alinear visión, ingeniería, seguridad, producto, testnet y narrativa institucional
No es	Código fuente, auditoría, especificación final de consenso ni promesa de rendimiento

Principios de redacción

- Distinguir siempre objetivos de ingeniería de métricas ya demostradas. 200K SFTPS es una meta arquitectónica que deberá validarse mediante benchmarks reproducibles.
- Utilizar “post-cuántico” para describir criptografía; la marca “Quantum Neural Blockchain” no implica que los validadores necesiten computadoras cuánticas.
- La IA no sustituye las reglas deterministas del protocolo. NeuroAgents analizan, atestiguan y ayudan a defender; la validez de consenso se mantiene verificable.
- La compatibilidad con ecosistemas legacy nunca debe convertir secp256k1 o Ed25519 en la autoridad final de cuentas nativas NEUROCHAIN.
- Una actualización de software nunca revierte arbitrariamente bloques ya finalizados.

Resumen ejecutivo

NEUROCHAIN como arquitectura integrada: no una colección de funciones, sino una única L1 diseñada alrededor de seis capacidades simultáneas.

Figura 1. Los seis pilares estratégicos integrados de NEUROCHAIN.

NEUROCHAIN se concibe como una Layer 1 soberana cuyo objetivo no es sobresalir en una única dimensión, sino integrar de forma nativa seguridad post-cuántica, inteligencia artificial en los nodos validadores, alto rendimiento, descentralización permissionless, semántica financiera ISO 20022 y una capacidad de defensa y actualización continua. La tesis es que estas propiedades deben diseñarse juntas desde Genesis, porque agregarlas posteriormente suele crear fricción, deuda técnica o dependencias que degradan las garantías originales.

La arquitectura propuesta diferencia el plano de datos, el plano de ejecución, el plano de consenso, el plano de inteligencia y el plano de seguridad. Esa separación interna permite que todo sea "nativo" sin obligar a que todo sea sincrónico. En particular, la validación criptográfica, el ordenamiento, la ejecución y la finalidad forman el hot path; el análisis profundo de IA, la telemetría, la indexación, la mayor parte de la lógica ISO, las simulaciones de actualización y la respuesta adaptativa operan en paralelo o de forma asincrónica siempre que la seguridad lo permita.

El objetivo de rendimiento se formula como 200.000 SFTPS —Secure Finalized Transactions Per Second— y no como una cifra de marketing de TPS brutas. Para contabilizarse como SFTPS, una operación deberá haber superado la validación criptográfica definida por el protocolo, haber sido ejecutada, incluida en un estado comprometido y finalizada por consenso. El número final dependerá de la implementación, del hardware, de la topología WAN, del tamaño de firmas PQC, de la carga de contratos y de la composición real de transacciones.

La seguridad post-cuántica se diseña desde el inicio mediante primitivas estandarizadas por NIST —ML-DSA para firmas, ML-KEM para establecimiento de secretos y SLH-DSA como alternativa basada en hashes para raíces críticas— combinadas con crypto-agility. La idea estratégica no es prometer que un algoritmo permanecerá seguro durante cien años, sino garantizar que la red pueda migrar de primitivas, suites criptográficas y formatos de autorización de manera gobernada y verificable.

Los validadores se proponen bajo un modelo de Proof of Stake permissionless para admisión económica y NeuroBFT para finalidad determinista. Cada validador incorpora un NeuroAgent local e independiente. El agente produce análisis y atestaciones firmadas, pero no obtiene autoridad para invalidar unilateralmente una operación protocolariamente válida. Esta separación busca evitar que un modelo probabilístico se convierta en árbitro absoluto del ledger.

La resiliencia evolutiva se agrupa bajo NeuroImmune. Un nodo que detecta y contiene un ataque puede emitir una cápsula de incidente firmada con evidencia, huellas y tests. Otros nodos reproducen el problema en entornos aislados; si la mitigación se valida, una regla de gobernanza/consenso autoriza un despliegue por canarios, shadow mode y A/B runtime. Si la nueva versión degrada salud o diverge en estado, el software puede volver al runtime anterior sin revertir bloques finalizados.

NEUROCHAIN se diseña también para operar en el ecosistema actual. La cuenta nativa se representa con un namespace propio —por ejemplo neuro1…— y su autoridad final permanece post-cuántica. Los prefijos 0x… pueden existir como alias o capa de compatibilidad EVM, pero no como fuente de seguridad de la cuenta nativa. WalletConnect, MetaMask Snaps, hardware wallets y custodios institucionales se integran mediante adaptadores que conservan esta separación.

Finalmente, NeuroISO trata ISO 20022 como lo que realmente es: un estándar de mensajería financiera. En lugar de publicar XML bancario completo on-chain, la red puede canonicalizar, cifrar y almacenar los mensajes bajo políticas de acceso, anclando en el ledger referencias, hashes, tipo de mensaje, autorización y evidencia de settlement. Con ello se busca una infraestructura capaz de servir tanto aplicaciones cripto-nativas como pagos, tokenización y flujos institucionales.

Mapa de decisiones fundacionales

Antes de entrar en los capítulos técnicos, esta matriz resume las decisiones que condicionan el resto del diseño. Sirve como referencia rápida para evitar que futuras optimizaciones contradigan la visión original.

Pregunta fundacional	Decisión conceptual	Condición de seguridad
¿PoW o PoS?	NeuroPoS para admisión + NeuroBFT para finalidad	La selección económica no sustituye las reglas BFT
¿IA manda sobre consenso?	No. NeuroAgents analizan y atestiguan	La validez base continúa determinista
¿Direcciones 0x nativas?	No. neuro1... es el namespace nativo	0x... queda como alias/compatibilidad
¿PQC añadido después?	No. PQC desde Genesis	Crypto-agility permite migrar en el futuro
¿ISO 20022 on-chain completo?	No. semántica + hash + refs + settlement	Payload sensible cifrado fuera del ledger
¿Update automático desde un nodo?	Nunca unilateral	Reproducción independiente + quorum + canary
¿Rollback de cadena?	No	Rollback de software, no de bloques finalizados
¿200K TPS como claim inicial?	No. target de ingeniería	Publicar solo SFTPS medido y reproducible
¿GPU potente = más votos?	No	AI capability no compra consensus power
¿Una sola implementación?	Solo al inicio	Multi-client es requisito de madurez

Figura de síntesis. Las decisiones fundacionales deben conservar los seis pilares simultáneamente.

Contenido

Índice estructural del dossier. Los estilos Heading permiten navegación directa desde el panel de Word.

PARTE I

VISIÓN, POSICIONAMIENTO Y PRINCIPIOS

Qué problema pretende resolver NEUROCHAIN y qué reglas condicionan toda decisión de ingeniería.

NEUROCHAIN • Quantum Neural Blockchain

Origen de la visión NEUROCHAIN

De una blockchain con IA a una red cognitiva, post-cuántica y evolutiva.

La conversación que dio forma a NEUROCHAIN comenzó con una idea sencilla pero exigente: si la inteligencia artificial va a formar parte de la infraestructura financiera del futuro, no debería vivir únicamente encima de una blockchain como una aplicación externa. El nodo que protege el ledger puede disponer de una capa inteligente local que observe, clasifique, aprenda y genere evidencia, siempre subordinada a reglas deterministas de consenso.

La segunda decisión fue rechazar el enfoque de "producto especializado". En lugar de crear una cadena solo para IA, una cadena solo para pagos o una cadena solo para seguridad post-cuántica, NEUROCHAIN se plantea como una L1 donde estas dimensiones formen parte de una arquitectura coherente. Esta amplitud aumenta la complejidad y, por eso, el diseño interno debe ser modular, medible y verificable.

La tercera decisión fue asumir desde Genesis que la red tendrá que cambiar. Una infraestructura destinada a durar décadas convivirá con nuevas familias criptográficas, vulnerabilidades desconocidas, nuevas generaciones de hardware, cambios en estándares financieros y modelos de IA que hoy no existen. La capacidad de actualizarse sin detener el ledger, probar versiones en shadow mode y regresar de software defectuoso se considera una propiedad estructural, no una herramienta de mantenimiento secundaria.

La cuarta decisión fue convertir la velocidad en una restricción permanente. Cada módulo incorporado debe declarar su coste de CPU, memoria, ancho de banda, almacenamiento y latencia. Si una función impide alcanzar el presupuesto de rendimiento, debe desacoplarse del hot path o rediseñarse. El objetivo de 200K SFTPS debe influir en serialización, batching, ejecución paralela, networking, storage y estructura de attestations desde el primer prototipo.

Por último, se decidió que descentralización y rendimiento no son objetivos intercambiables. Una red que logre cifras extraordinarias obligando a cada validador a adquirir infraestructura prohibitiva habrá cambiado throughput por concentración. NEUROCHAIN debe buscar rendimiento por paralelismo, committees, data-plane eficiente y aceleración opcional, manteniendo requisitos razonables para un validador estándar.

Tesis central

Tesis — La diferenciación de NEUROCHAIN no reside en que cada una de sus capacidades sea inédita por separado, sino en diseñarlas como propiedades simultáneas de una misma L1, con garantías explícitas para evitar que una destruya a las demás.

Principios de diseño no negociables

Las reglas que deben sobrevivir a cambios de lenguaje, cliente, hardware y proveedor.

Principio	Implicación arquitectónica
Seguridad determinista	La IA puede recomendar, puntuar y atestiguar; la validez básica del ledger debe seguir reglas reproducibles por clientes independientes.
PQC nativo	Las cuentas y validadores nativos no dependen de firmas legacy como autoridad final.
Crypto-agility	Algoritmos y suites se versionan y migran; ninguna primitiva queda embebida como una dependencia eterna.
Hot path mínimo	Cada etapa sincrónica debe justificar su presencia. Análisis profundos, indexación y actualizaciones se desplazan a planos paralelos cuando es seguro.
Descentralización económica	El mecanismo de stake debe evitar que la simple acumulación de capital compre control ilimitado del consenso.
Observabilidad verificable	Bloques, attestations, upgrades y health metrics deben generar evidencia auditable sin exponer secretos.
Privacidad financiera	Integrar ISO 20022 no significa publicar datos bancarios sensibles en un ledger público.
No rollback del ledger	Un rollback de software nunca debe significar reescribir silenciosamente un historial finalizado.
Clientes múltiples	La madurez de mainnet debe incluir implementaciones independientes de la especificación para reducir riesgo de monocultura.
Medición antes de claim	Velocidad, finality, seguridad y descentralización se publican con metodología reproducible y contexto.

El principio operativo

La frase que resume la filosofía de NEUROCHAIN es: “Everything native. Nothing unnecessarily synchronous.” Una función puede ser protocol-native sin bloquear cada transacción. Esta distinción permite integrar IA, ISO 20022, observabilidad y resiliencia sin convertir el camino crítico en una cadena secuencial de servicios lentos.

Figura 2. Hot path propuesto y funciones deliberadamente desacopladas.

04

Qué significa “Quantum Neural Blockchain”

Terminología de marca frente a afirmaciones técnicas.

“Quantum Neural Blockchain” es una denominación de posicionamiento. Técnicamente, el término relevante es post-quantum cryptography (PQC): algoritmos diseñados para resistir las clases de ataques que serían posibles con computadores cuánticos de gran escala. NEUROCHAIN no requiere un computador cuántico para operar y no debe insinuar que utiliza “computación cuántica” cuando la función real es criptografía post-cuántica.

La palabra Neural se relaciona con la distribución de NeuroAgents a través de la red. Cada validador puede ejecutar un agente local que analiza actividad, produce attestations y participa en un sistema de aprendizaje defensivo distribuido. La analogía neural es conceptual: muchos nodos autónomos observan, comunican evidencia y fortalecen la red, pero el consenso continúa bajo reglas explícitas.

Esta precisión lingüística es importante para inversores, auditores, reguladores y desarrolladores. Claims amplios como “100% quantum” o “la blockchain más segura del mundo” deben sustituirse por afirmaciones comprobables: qué primitives se usan, qué parte del protocolo está protegida, qué algoritmos son versionables, qué benchmarks se han ejecutado y qué auditorías independientes han validado cada capa.

Regla de comunicación — Usar superlativos solo después de contar con testnet pública, metodología publicada, auditorías y resultados reproducibles. La narrativa debe ser ambiciosa, pero la evidencia debe ir primero.

PARTE II

ARQUITECTURA DEL PROTOCOLO

Cómo conviven datos, ejecución, consenso, IA, finanzas y seguridad sin formar un monolito.

NEUROCHAIN • Quantum Neural Blockchain

Arquitectura general por capas

Una sola L1, internamente desacoplada.

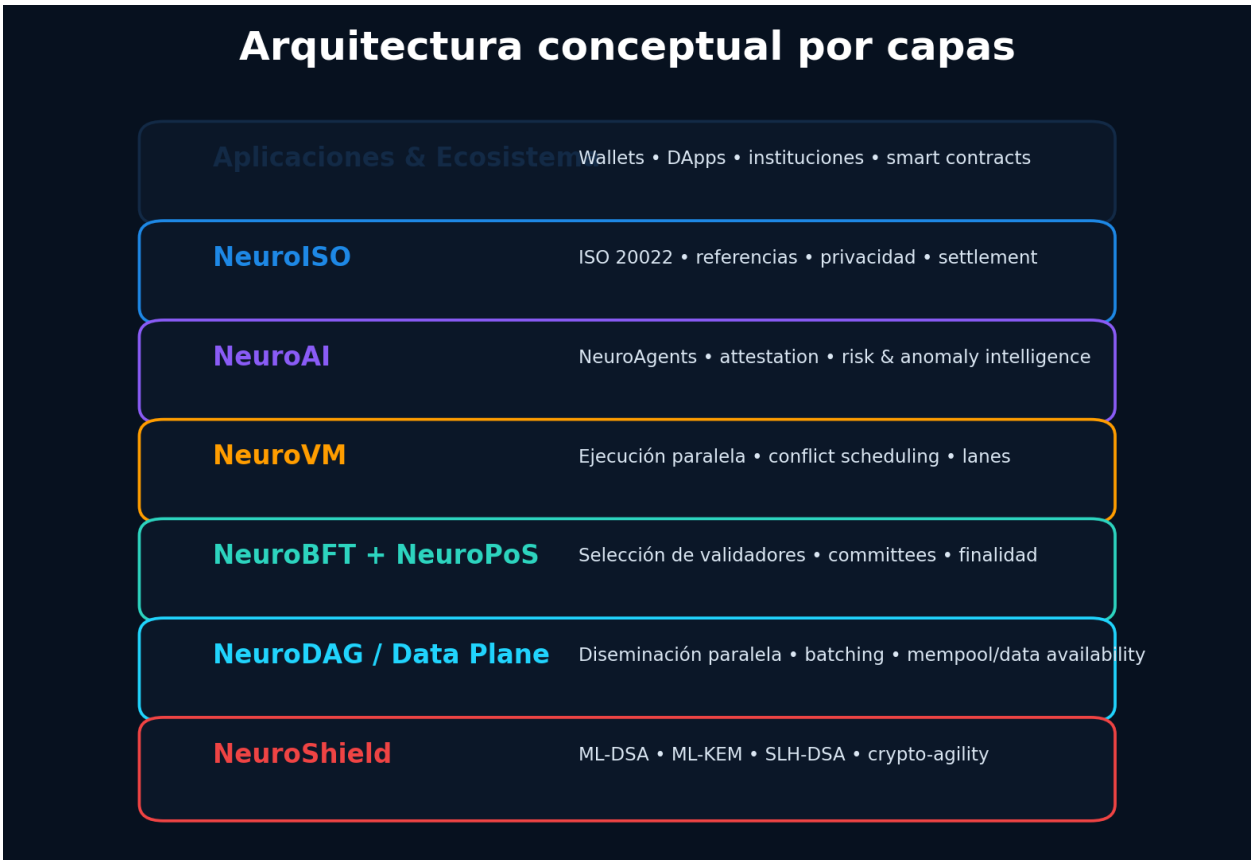

Figura 3. Vista conceptual por capas de NEUROCHAIN.

NEUROCHAIN debe presentarse como una única blockchain soberana. La modularidad descrita en este documento es interna: sirve para organizar responsabilidades, performance budgets, testing y evolución. No implica fragmentar la experiencia de usuario en múltiples redes ni obligar a los desarrolladores a entender subsistemas diferentes para una transferencia normal.

NeuroShield establece las primitivas criptográficas, identidades y mecanismos de migración. NeuroDAG constituye el data plane que recibe y distribuye lotes de transacciones. NeuroPoS determina el conjunto elegible de validadores y NeuroBFT finaliza decisiones. NeuroVM ejecuta operaciones y contratos con paralelismo. NeuroAI aporta inteligencia local y attestations. NeuroISO mapea semántica financiera. Finalmente, las aplicaciones interactúan mediante RPC, SDK, wallet interoperability y explorer.

Cada capa debe exponer interfaces versionadas y observables. La versión de un modelo AI no tiene que coincidir con la versión del protocolo; una actualización de una política de seguridad no debe

exigir un hard fork; una migración de suite criptográfica debe poder coexistir con una ventana de transición; una nueva familia ISO debe incorporarse sin alterar el consenso básico. Esta independencia reduce el radio de impacto de los cambios.

Versionado recomendado

Componente	Ejemplo de versión	Razón de separación
Protocol	NP-1.0	Reglas de validez y estado
Node client	neurochaind 1.4.2	Implementación de software
Consensus	NeuroBFT 1.1	Reglas de round/finality
Crypto suite	NEURO-PQ-2026	Primitivas autorizadas
AI policy	NAP-142	Formato/criterios de attestation
Security policy	NSP-8821	Defensas operativas
ISO schema pack	NISO-2026Q3	Mensajes financieros soportados

Anatomía del nodo validador

El validador como unidad criptográfica, de consenso, ejecución e inteligencia.

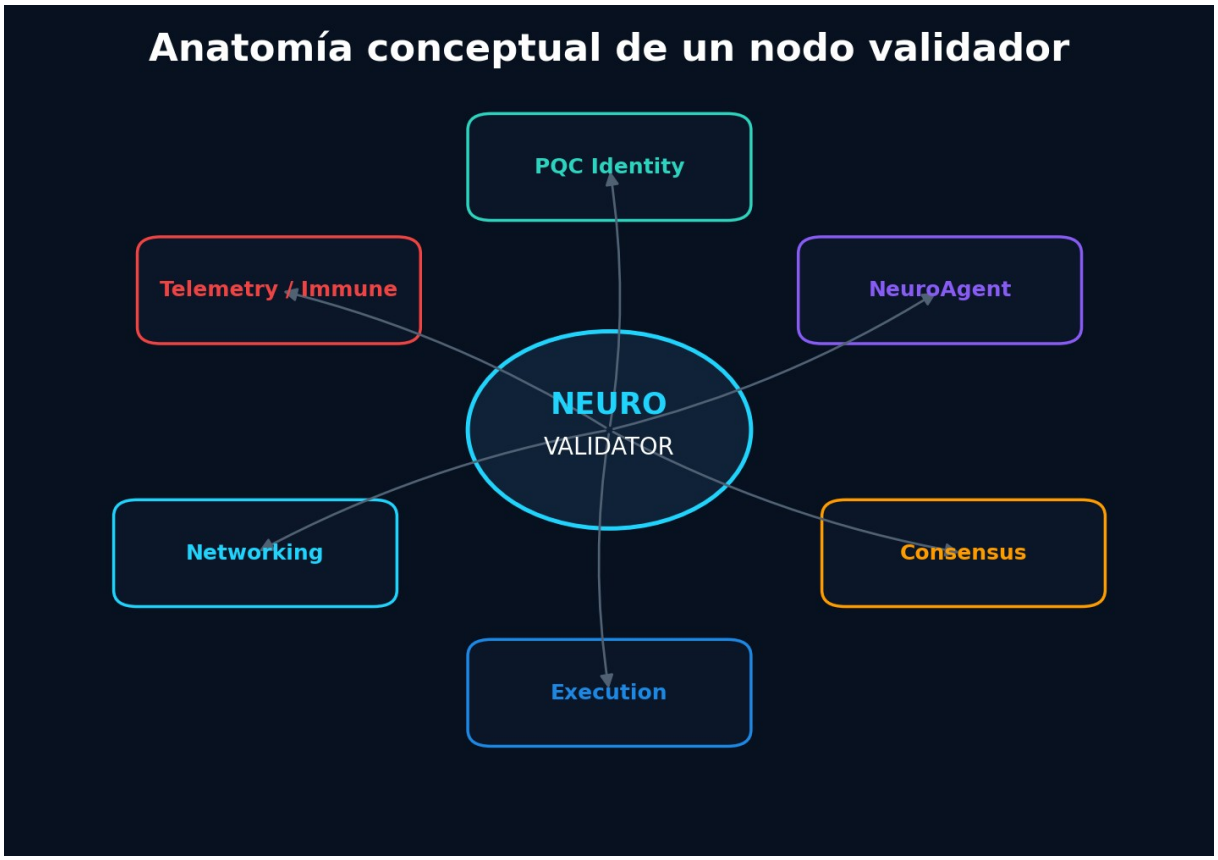

Figura 4. Componentes de alto nivel de un NeuroValidator.

Un validador NEUROCHAIN no se define por un único proceso de firma. Es un conjunto de servicios controlados que comparten identidad y estado: networking, verificación PQC, ejecución, participación en consenso, NeuroAgent, observabilidad y módulo NeuroImmune. En producción, estos componentes pueden aislarse en procesos o sandboxes distintos para reducir privilegios y contener fallos.

La identidad de consenso debe ser post-cuántica y separarse de las claves de operador, retiro, gobernanza o actualización. Las claves online deberían rotar por epoch o por periodos definidos, autorizadas por raíces de mayor seguridad que permanecen fuera de línea. Este esquema limita el daño de una intrusión en un servidor en ejecución.

El NeuroAgent consume datos estructurados del nodo: características de transacciones, comportamiento de peers, desviaciones de latencia, anomalías de recursos y señales de seguridad.

Su salida se normaliza en attestations pequeñas y firmadas. El modelo completo, prompts internos, heurísticas propietarias o datasets no necesitan publicarse para que la attestation sea verificable.

Para descentralización, el protocolo no debe exigir que todos utilicen el mismo proveedor de IA. Se define un contrato de interoperabilidad: estructura de entrada, estructura de salida, políticas mínimas, latency budget y reglas de evidencia. Un modelo local pequeño y uno empresarial más sofisticado pueden coexistir sin que el segundo reciba votos adicionales por ser más caro.

Separación de privilegios

- Consensus signer: capacidad limitada a mensajes de consenso y bloques.
- PQC root: offline o altamente aislada; autoriza rotaciones, no participa en cada bloque.
- NeuroAgent: sin acceso directo a claves privadas de consenso.
- Updater: solo acepta artefactos autorizados, reproducibles y firmados.
- Explorer/indexer: lectura; nunca forma parte de la seguridad de consenso.
- Administración: políticas auditadas y, en mainnet, gobernanza distribuida.

Modelo de cuentas, direcciones y objetos nativos

Identidad NEUROCHAIN diferenciada, legible y crypto-agile.

El prefijo 0x… pertenece a convenciones EVM y no debería representar la identidad nativa de NEUROCHAIN. Se propone un namespace legible como neuro1… para cuentas, neuroval1… para validadores y prefijos separados para identificadores de transacciones o representaciones amigables de bloque. El formato final deberá especificar checksum, codificación, longitud y capacidad de versionar tipos de cuenta.

La dirección no debe codificar de forma irreversible una única familia criptográfica. Una cuenta puede apuntar a una política de autenticación versionada en estado: suite de firma, versión de clave, reglas de recuperación, multisig y autorizaciones de sesión. Esto convierte la cuenta en una abstracción durable mientras las primitivas evolucionan.

Para interoperabilidad, una cuenta puede registrar aliases legacy —por ejemplo una dirección EVM — con propósito de descubrimiento, autorización secundaria o UX. Sin embargo, un alias secp256k1 no se convierte por defecto en una autorización suficiente para mover fondos nativos PQ. La capa de compatibilidad debe traducir la intención del usuario hacia una autorización aceptada por la política nativa.

Objeto	Formato conceptual	Uso
Cuenta	neuro1…	Cuenta nativa / autoridad PQ
Validador	neuroval1…	Identidad del validator set
Transacción	ntx1…	Identificador legible de TX
Bloque	nblk1…	Representación legible / explorer
Alias EVM	0x…	Compatibilidad, no autoridad nativa por defecto

Flujo de una transacción

Desde la intención del usuario hasta un bloque finalizado.

Figura 5. Camino crítico conceptual de una transacción.

Una transacción entra por RPC, wallet o gateway y se somete primero a validaciones baratas: formato, chain identifier, tamaño, nonce, disponibilidad de saldo, límites de recursos y política de cuenta. Los filtros económicos y de rate limiting deben impedir que firmas PQC costosas se utilicen como vector de denegación de servicio.

La verificación criptográfica confirma la autorización según la suite de la cuenta. Cuando sea posible, el motor utiliza batching, caches de claves públicas y técnicas de verificación paralela. En paralelo, el NeuroAgent fast path puede calcular una puntuación de riesgo y NeuroISO puede resolver metadatos o referencias sin bloquear innecesariamente el ordenamiento.

NeuroDAG distribuye los lotes y desacopla el movimiento de datos de la decisión de orden. NeuroVM determina qué operaciones son independientes, programa ejecución paralela y serializa únicamente los conflictos. NeuroBFT alcanza la finalidad y se genera un commitment de estado. El explorer, indexadores y análisis profundos consumen eventos después de la finalización.

La latencia de una transacción no debe sumarse ingenuamente como “PQC + IA + ISO + ejecución + consenso”. La arquitectura intenta solapar trabajo y reservar la sincronía únicamente para las dependencias que afectan la seguridad. Este principio será central en cualquier intento de aproximarse a 200K SFTPS.

NeuroDAG y plano de datos

Mover información con eficiencia antes de decidir su orden final.

En redes de alto rendimiento, la diseminación de transacciones puede convertirse en un cuello de botella incluso antes de ejecutar contratos. NeuroDAG representa la intención de separar el data plane del ordering plane, utilizando batches, referencias criptográficas y estructuras de disponibilidad que permitan a los validadores trabajar sobre datos ya distribuidos.

El objetivo no es imponer un DAG específico en esta etapa, sino adoptar una arquitectura que pueda beneficiarse de investigación BFT moderna. La implementación final deberá comparar alternativas mediante simulación y testnet WAN: tamaños de batch, latencia entre regiones, pérdida de paquetes, presión de memoria, comportamiento con peers lentos y resistencia a spam.

Para evitar que el data plane crezca sin control, deben existir presupuestos de bytes por segundo, políticas de backpressure, prioridad por fees o clases de servicio, límites por peer y mecanismos de recuperación. Una red de 200K SFTPS no se construye solamente optimizando CPU; el ancho de banda y la amplificación de mensajes pueden dominar el sistema.

Criterios de éxito del data plane

- Alta utilización del ancho de banda sin congestión explosiva.
- Batches verificables y fáciles de repropagar.
- Recuperación rápida de nodos rezagados.
- Priorización anti-spam que no cree censura discrecional.
- Observabilidad por batch, peer y región.
- Compatibilidad con committees y ejecución paralela.

NeuroVM y ejecución paralela

La escalabilidad nace de no serializar lo que no tiene dependencia.

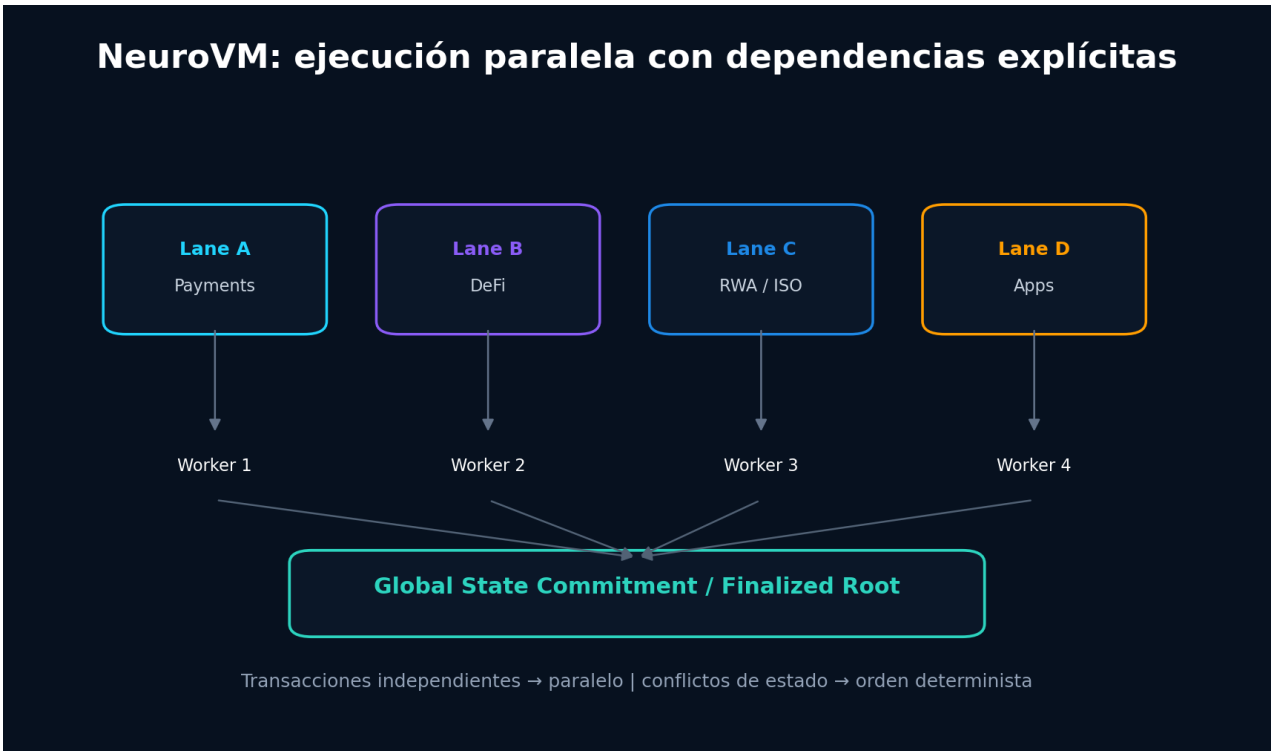

Figura 6. Ejecución por lanes y commitment global.

La ejecución secuencial obliga a que dos transacciones independientes esperen una por otra. NEUROCHAIN debe declarar o inferir de forma segura los conjuntos de estado que una operación lee y escribe, permitiendo que el scheduler agrupe operaciones no conflictivas en workers paralelos. Cuando dos operaciones compiten sobre la misma cuenta o contrato, se establece un orden determinista.

El concepto de lanes no debe interpretarse necesariamente como sharding rígido por industria. Puede funcionar como unidades de planificación que cambian con la carga y el grafo de dependencias. Una lane de pagos puede convivir con lanes de contratos, RWA, ISO o aplicaciones, mientras todas convergen en commitments que el consenso puede verificar.

El paralelismo también debe existir en la verificación de firmas, serialización, acceso a base de datos, construcción de índices y recepción de red. Una arquitectura que solo paraleliza la VM pero mantiene un storage lock global seguirá limitada. Por ello el benchmark debe perfilar CPU, I/O, locks, cachés, GC, memoria y ancho de banda por separado.

El objetivo de mainnet no es que todos los validadores ejecuten exactamente el mismo número de workers. El scheduler debe detectar los recursos disponibles y mantener resultados deterministas. Una máquina con 32 cores puede procesar más trabajo en paralelo que una de 16, pero ambas deben llegar al mismo estado final y seguir siendo participantes válidos bajo requisitos mínimos definidos.

PARTE III

CONSENSO, VALIDADORES Y DESCENTRALIZACIÓN

Cómo se entra a la red, cómo se limita el poder y cómo se finalizan bloques.

NEUROCHAIN • Quantum Neural Blockchain

Por qué Proof of Stake y no Proof of Work

Usar el cómputo para seguridad, ejecución e IA, no para una carrera de hashing.

NEUROCHAIN propone Proof of Stake como mecanismo de admisión y seguridad económica. La razón principal es que la GPU, CPU y ancho de banda de un nodo deben dedicarse a validar, ejecutar, propagar datos y alimentar NeuroAgents; no a competir en un proceso de minería que consuma recursos sin aportar directamente a estas funciones.

PoS no resuelve por sí solo el consenso. Define quién tiene garantía económica y bajo qué condiciones participa. NeuroBFT define cómo el conjunto activo intercambia votos y alcanza finalidad. Mantener esta separación conceptual permite ajustar staking, delegación o caps económicos sin reescribir las reglas fundamentales de ordenamiento.

El stake mínimo de mainnet no debe fijarse prematuramente en una cantidad nominal de NEURO. Si el precio del activo cambia en órdenes de magnitud, un requisito fijo puede hacer que validar sea trivialmente barato o prohibitivo. El protocolo puede utilizar objetivos económicos, mecanismos de ajuste y límites de effective stake para reducir concentración.

Lifecycle de un validador

Full node → candidato → stake → activación → operación → salida.

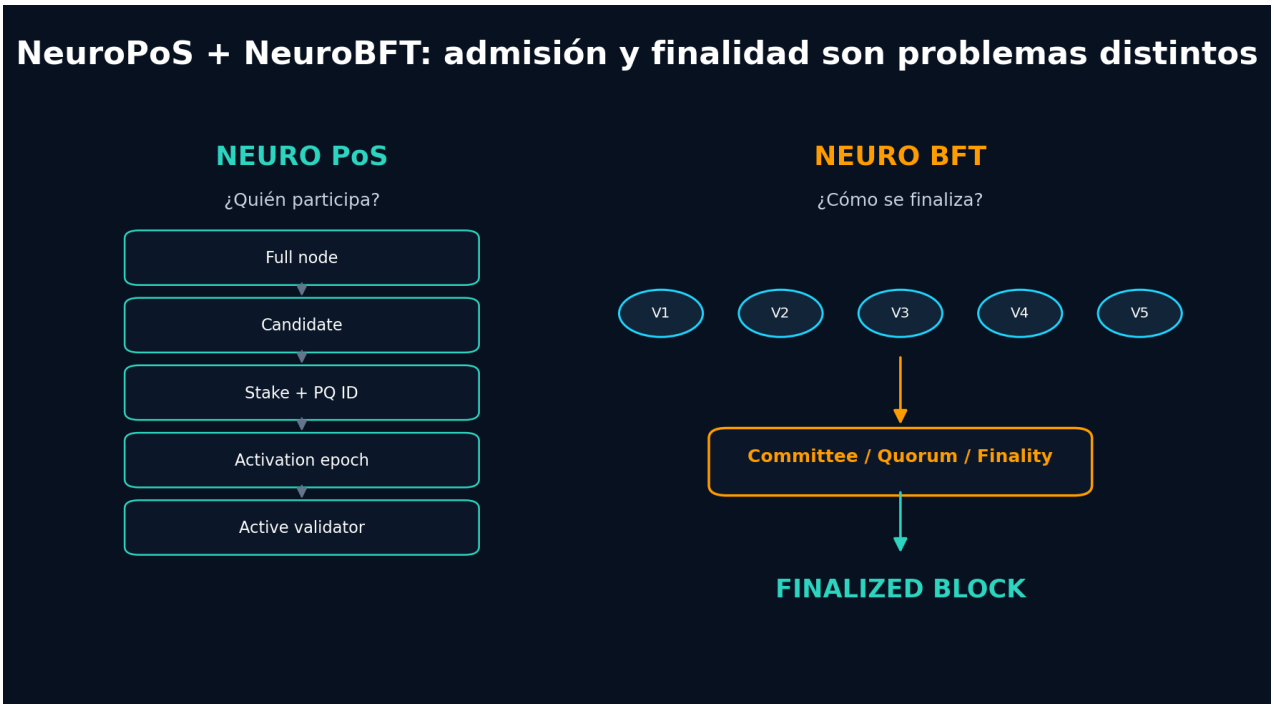

Figura 7. NeuroPoS selecciona participación; NeuroBFT finaliza.

1. Instalar un cliente compatible y sincronizar el ledger como full node.
2. Generar identidad PQC del validador y separar claves online de raíces de control.
3. Registrar la candidatura y demostrar cumplimiento de requisitos de protocolo.
4. Bloquear stake o recibir delegación según el modelo económico vigente.
5. Esperar la ventana de activación definida por epoch para evitar cambios abruptos del validator set.
6. Participar en committees, propuesta y votación; emitir attestations AI y telemetría verificable.
7. Rotar claves y software bajo políticas de actualización segura.
8. Solicitar salida y respetar un periodo de unbonding que permita sancionar violaciones demostrables.

Slashing: hechos demostrables, no opiniones de IA

El slashing debe reservarse para conductas que puedan probarse criptográficamente: double-sign, votos contradictorios, firma de bloques inválidos, mensajes de consenso incompatibles o manipulación demostrada. Un NeuroAgent puede equivocarse en una predicción probabilística; esa equivocación no debe tratarse automáticamente como una infracción económica.

NeuroBFT y committees

Finalidad rápida sin obligar a miles de nodos a hablar con todos en cada ronda.

Una red con diez validadores puede tolerar comunicaciones densas; una con diez mil no. NEUROCHAIN debe permitir una población amplia de validadores y seleccionar committees mediante mecanismos criptográficos verificables. Los committees participan en rondas de consenso y rotan para impedir que un grupo fijo concentre el poder durante periodos extensos.

La especificación final de NeuroBFT debe apoyarse en investigación BFT revisada y en pruebas formales. En esta fase, el nombre representa un diseño objetivo: finalidad determinista, tolerancia bizantina, comunicación eficiente, compatibilidad con DAG data-plane, rotación de committees y soporte de upgrades versionados.

Los NeuroAgents no aumentan el peso de voto. Un validador con un modelo de IA de mayor tamaño no obtiene más poder. La inteligencia se convierte en información adicional y defensa, mientras que la regla de quorum depende del stake efectivo, la selección protocolaria y las restricciones de descentralización definidas.

Para alcanzar latencias cercanas a un segundo en WAN, será necesario medir cuidadosamente el número de hops, tamaño de certificados, agregación de votos, firmas PQC, latencia interregional y tamaño de committee. Las metas deben probarse con nodos distribuidos físicamente; localhost no demuestra finalidad global.

Descentralización económica y técnica

Evitar que “muchos nodos” oculte concentración real.

La descentralización tiene dimensiones diferentes: número de validadores, distribución geográfica, diversidad de proveedores cloud, diversidad de clientes, concentración de stake, dependencia de un proveedor de IA, distribución de infraestructura RPC y acceso a hardware. NEUROCHAIN debe publicar indicadores para cada dimensión en lugar de un único número de nodos.

Un effective stake cap puede impedir que un único validador convierta capital ilimitado en poder de consenso lineal. El exceso de stake podría delegarse, distribuir rewards o quedar económicamente reconocido sin incrementar el peso por encima de un límite. El diseño final requerirá simulaciones para evitar incentivos a dividir artificialmente una entidad en múltiples identidades.

La diversidad de clientes es crítica. Una mainnet madura debería disponer de al menos dos implementaciones independientes de la especificación y avanzar hacia tres o más. Un bug en un cliente no debería tumbar toda la red. Los releases deben incluir matrices de compatibilidad y pruebas de consenso cruzadas.

También debe evitarse una dependencia AI monocultural. La capa de NeuroAgents debe aceptar implementaciones diversas siempre que produzcan outputs válidos. Un modelo de referencia puede facilitar adopción, pero la red no debe dejar de funcionar si un proveedor de IA desaparece o cambia condiciones.

PARTE IV

RENDIMIENTO Y ESCALABILIDAD

Diseñar para 200K SFTPS sin convertir la red en un datacenter centralizado.

NEUROCHAIN • Quantum Neural Blockchain

200.000 SFTPS como objetivo de ingeniería

Definir qué se mide antes de perseguir el número.

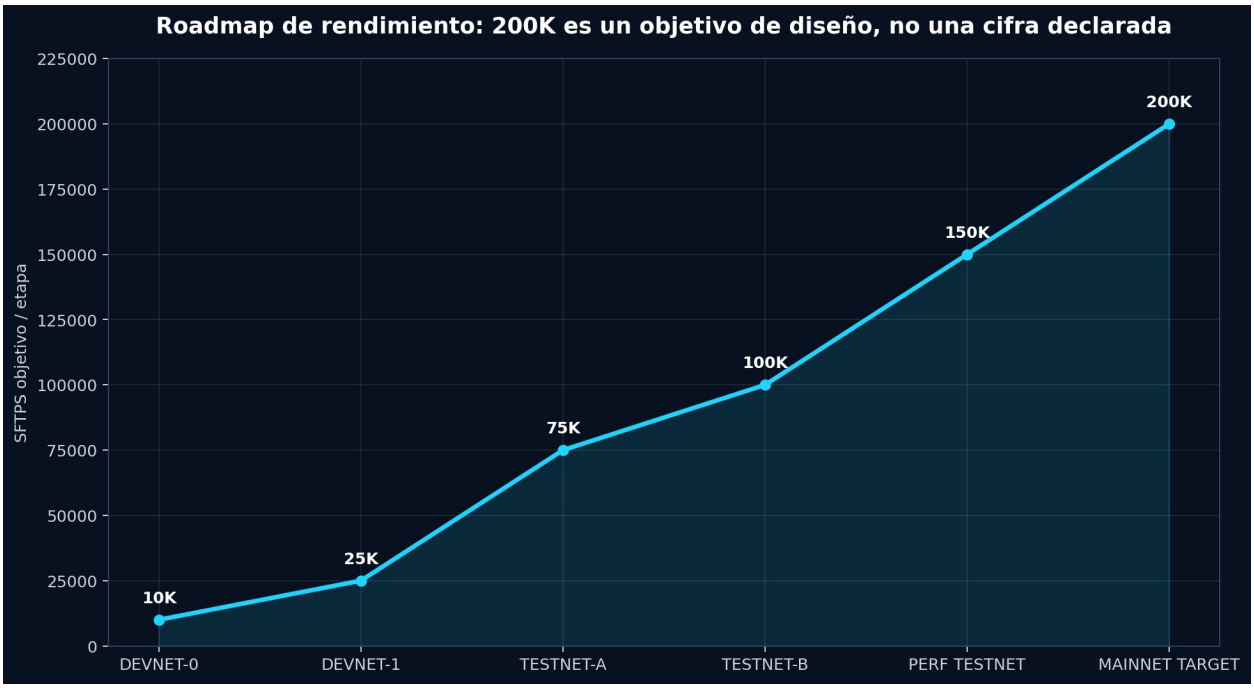

Figura 8. Roadmap indicativo de rendimiento por etapas.

El objetivo de 200.000 no debe tratarse como una promesa inicial. Se utiliza como constraint de arquitectura. Cada decisión de formato de transacción, verificación PQC, scheduling, base de datos, networking, tamaño de committee o AI fast path debe evaluarse contra el presupuesto de throughput y latencia.

SFTPS significa Secure Finalized Transactions Per Second. Una transacción cuenta solo cuando está autorizada, ejecutada, incorporada al commitment de estado y finalizada. Los benchmarks deben declarar además composición de carga: transferencias simples, contratos con conflictos, ISO metadata, firmas PQC, transacciones inválidas, tamaño promedio, porcentaje de AI deep-path y distribución geográfica.

La meta debe medirse como throughput sostenido, no como pico de segundos. Un benchmark serio incluirá periodos de 30–60 minutos, p50/p95/p99 de finality, CPU/GPU/RAM, bytes por transacción, ancho de banda por nodo, tasa de retransmisión, crecimiento del state y desempeño durante caída de validadores.

La evolución planteada es incremental: DEVNET-0 prioriza corrección y puede comenzar con miles de TPS. Las siguientes fases incrementan carga, número de regiones y adversarial testing. Si una

etapa no alcanza su meta, se perfila el cuello de botella y se corrige antes de incrementar complejidad.

Métricas mínimas de benchmark

Métrica	Qué demuestra
SFTPS sostenidas	Capacidad real bajo garantías completas
Finality p50/p95/p99	Experiencia y cola de latencia
CPU por nodo	Coste de ejecución/PQC/consenso
GPU utilization	Coste del NeuroAgent
Bytes/TX	Presión de red y almacenamiento
State growth	Sostenibilidad a largo plazo
Fault mode throughput	Degradación con validadores caídos
Invalid TX rejection	Resistencia a spam/adversarial load

AI fast path y deep path

La inteligencia no puede bloquear 200.000 operaciones por segundo.

El error más evidente sería llamar a un LLM grande para cada transacción y esperar su respuesta antes de continuar. El NeuroAgent debe disponer de un fast path de milisegundos o menos basado en features, modelos especializados, reglas de seguridad y cachés. Solo un porcentaje pequeño de eventos activa análisis profundo.

Una transferencia rutinaria puede recibir una attestation mínima con risk score, policy version y evidence hash. Un bridge, una operación institucional de gran valor, un patrón de drenaje o una anomalía de contrato puede activar deep path. Dependiendo del caso, el análisis profundo puede influir en una política explícitamente opt-in, en un módulo regulado o en alertas, pero no convertir una opinión del modelo en censura arbitraria.

El formato de attestation debe ser compacto. No se almacena razonamiento textual completo on-chain. Se comprometen identificador de agente/modelo, política, decisión, puntuación, hashes de evidencia y firma. Los artefactos extensos pueden almacenarse en sistemas verificables externos con controles de privacidad.

Escalabilidad horizontal: lanes, workers y estado

Aumentar capacidad agregando recursos, no elevando un lock global.

La escalabilidad de NEUROCHAIN debe existir en varios niveles: recepción de red, verificación criptográfica, execution workers, almacenamiento, indexación y API. Si cualquiera de estos componentes continúa siendo estrictamente monohilo, se convertirá en el techo del sistema aunque los otros módulos escalen.

Las execution lanes permiten repartir trabajo por conjuntos de estado y tipo de carga. No es necesario asociarlas permanentemente a una industria. El scheduler puede formar grupos dinámicos y mover carga según conflictos. El commitment global asegura que el sistema continúa siendo una sola L1 desde el punto de vista del usuario.

La base de datos debe diseñarse con acceso concurrente, snapshots, versioned state y separación entre estado caliente e historia. Los nodos pueden tener roles diferentes —validator, archival, indexer— sin que el validator estándar necesite conservar índices analíticos completos.

En el plano de red, la diseminación de batches y la selección de committees deben reducir fan-out. Se evaluarán estrategias de compresión, erasure coding, conexiones persistentes, QUIC u otros transportes compatibles con la capa PQC, pero la elección definitiva solo se realizará mediante benchmark y revisión de seguridad.

Requisitos de hardware y descentralización

Rendimiento sin convertir el validador en un servidor inaccesible.

Un objetivo de 200K SFTPS puede lograrse de forma artificial exigiendo hardware extremo. NEUROCHAIN necesita un perfil de “standard validator” razonable para su época: CPU multinúcleo, 64–128 GB RAM, NVMe y conectividad de 1–2.5 Gbps como orden de magnitud inicial. La GPU puede recomendarse para NeuroAgent avanzado, pero no debería comprar peso de consenso.

Los AI accelerators pueden separarse lógicamente del consensus core. Un validador con GPU más potente ejecuta modelos más profundos, pero el protocolo continúa aceptando un agente de referencia ligero que cumpla el contrato mínimo. Esto reduce la barrera de entrada y conserva diversidad de operadores.

La testnet debe incluir deliberadamente hardware heterogéneo: workstations, servidores cloud, bare metal, distintas regiones y nodos domésticos. La degradación de rendimiento se mide y se utilizan requisitos mínimos basados en datos, no en preferencias del equipo de ingeniería.

PARTE V

SEGURIDAD POST-CUÁNTICA Y CONTINUIDAD A 100 AÑOS

PQC desde Genesis, crypto-agility, múltiples capas de control y diseño para migrar.

NEUROCHAIN • Quantum Neural Blockchain

NeuroShield y criptografía post-cuántica

Primitivas nativas sin convertir una única elección en destino permanente.

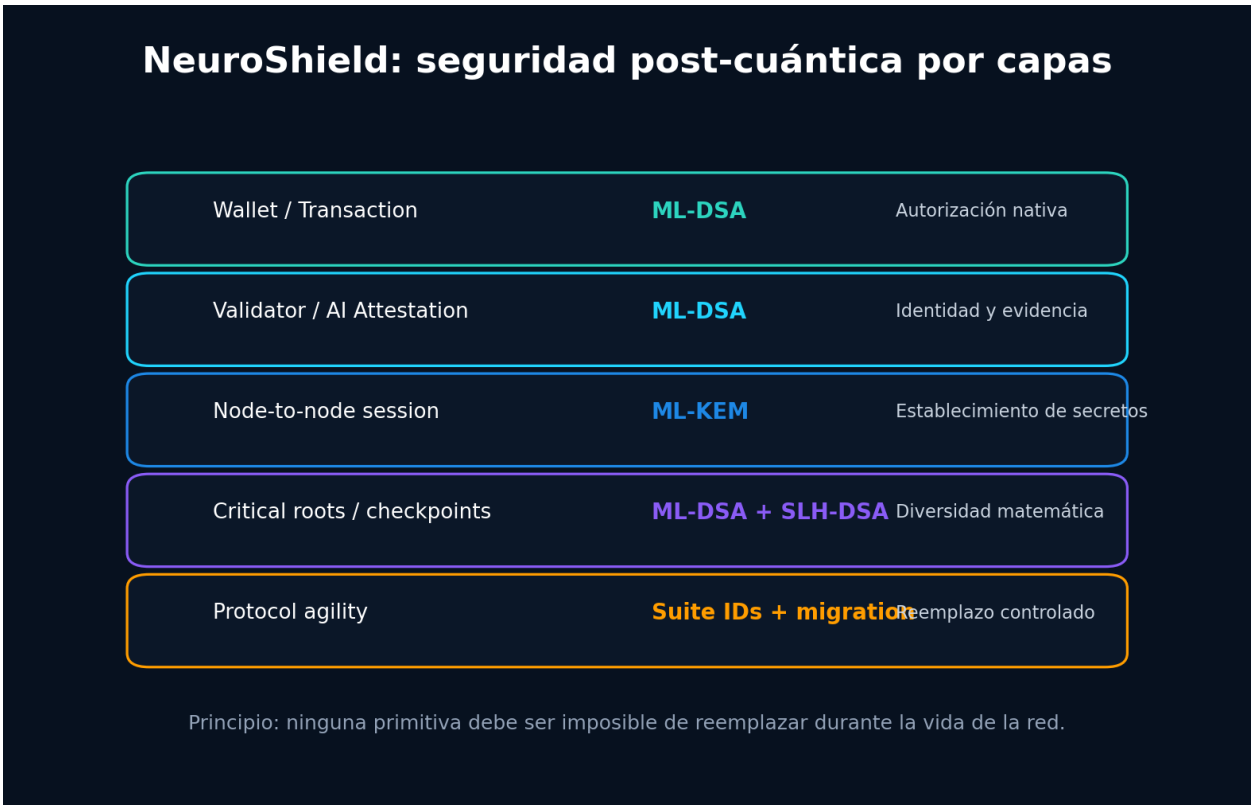

Figura 9. Capas PQC conceptuales de NeuroShield.

Los estándares FIPS 203, 204 y 205 de NIST proporcionan una base para diseñar la primera suite: ML-KEM para establecimiento de secretos, ML-DSA para firmas y SLH-DSA como firma basada en hashes. La selección de niveles concretos —por ejemplo ML-DSA-44/65/87— debe depender de benchmark, lifetime de claves, criticidad y análisis de seguridad, no de una preferencia fija en este documento.

La identidad de usuario, la identidad de validador y las attestations AI pueden utilizar firmas PQC. Las conexiones entre nodos incorporan establecimiento de claves PQ. Las operaciones críticas —raíces de gobernanza, checkpoints, autorizaciones de suite— pueden exigir diversidad criptográfica o políticas multisig que reduzcan el riesgo de una sola familia matemática.

PQC introduce firmas y claves más grandes que esquemas legacy; ese overhead es relevante para 200K SFTPS. NEUROCHAIN debe registrar claves públicas una vez cuando sea posible, reducir repetición de metadata, aprovechar batching seguro y medir bytes por transacción como una métrica de primer nivel.

La seguridad post-cuántica también debe cubrir backups, snapshot signing, actualización de software, repositorios de artefactos y canales operativos. Una red que firma bloques con ML-DSA pero distribuye binarios mediante una cadena de suministro vulnerable no puede presentarse como end-to-end secure.

Crypto-agility

La verdadera estrategia de seguridad centenaria.

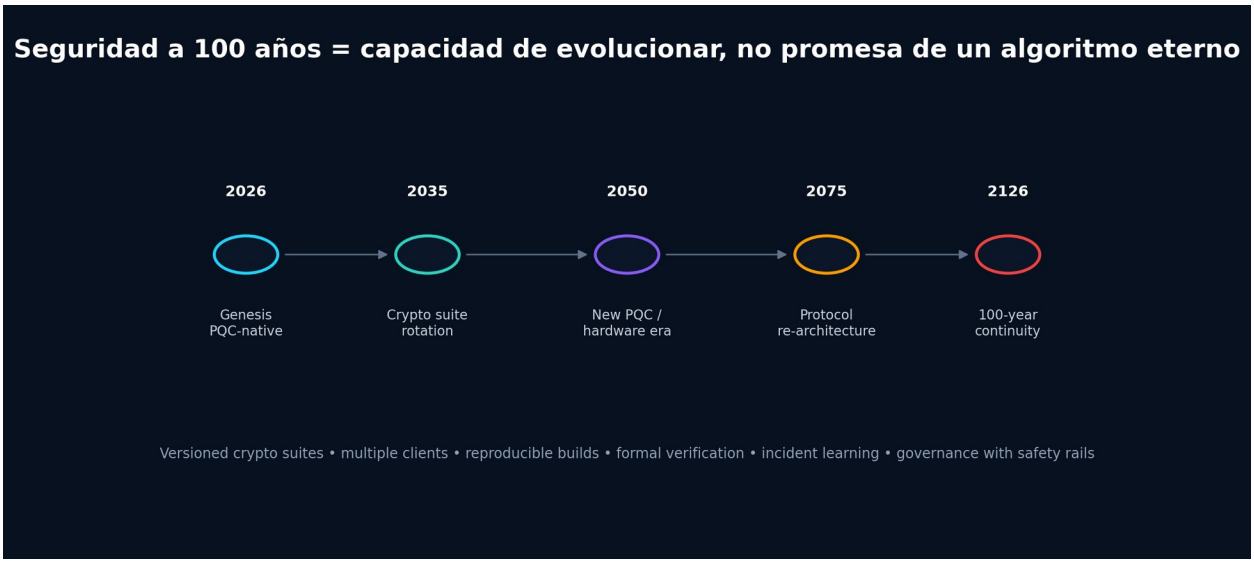

Figura 10. La continuidad se diseña como capacidad de migración.

No existe una forma responsable de garantizar hoy que una primitiva concreta seguirá siendo adecuada en 2126. La promesa defendible es otra: NEUROCHAIN debe saber sustituir algoritmos sin perder la continuidad del ledger, y debe practicar esa migración antes de que exista una emergencia.

Las transacciones y cuentas pueden declarar suite IDs; el protocolo mantiene una registry de suites activas, deprecadas y prohibidas. Una actualización puede abrir una ventana dual donde cuentas antiguas roten claves, mientras nuevas cuentas nacen bajo la suite más reciente. Los checkpoints y governance roots se rotan bajo procedimientos más estrictos.

La crypto-agility se prueba en testnet mediante “fire drills”: se marca una suite como vulnerable de forma simulada, se activa otra, se miden latencias, migración de cuentas, compatibilidad de wallets y sincronización de clientes. Así la capacidad de cambio deja de ser una idea teórica.

Gestión de claves y superficies críticas

Separar online, offline, epoch y recovery.

La seguridad de un validador depende tanto de la primitive como de la custodia. Un diseño recomendado utiliza una root key offline que autoriza claves online de epoch o de corta vida. Si un servidor operativo es comprometido, el atacante obtiene una ventana limitada y no la raíz permanente del validador.

Las wallets de usuario deben disponer de políticas de recuperación que no reintroduzcan una clave legacy débil como bypass universal. Recovery puede utilizar multisig PQ, guardians, time locks o políticas de smart account, pero siempre debe declararse explícitamente qué nivel de seguridad ofrece.

Las claves de upgrade, gobernanza y treasury deben permanecer fuera de los servidores de consenso. La red no debe aceptar una “master key” unilateral capaz de reescribir estado. Emergencias se gestionan mediante políticas de quorum, timelocks adaptativos y capacidades específicas con alcance reducido.

Múltiples clientes, formal verification y supply chain

La seguridad más allá de la criptografía.

Una vulnerabilidad lógica puede ser más peligrosa que una primitive rota. NEUROCHAIN debe evolucionar hacia múltiples clientes independientes que implementen una especificación común. El cliente inicial puede estar en Go o Rust; una segunda implementación independiente debe convertirse en milestone de pre-mainnet o early-mainnet.

Los componentes críticos —state transition, signature policy, consensus safety, upgrade authorization— son candidatos a especificación formal, model checking y property-based testing. No todo el sistema necesita probarse formalmente para obtener valor: concentrarse en invariantes de seguridad reduce áreas donde una divergencia puede romper el ledger.

Los builds de releases deben ser reproducibles. Múltiples builders independientes compilan el mismo commit y comparan hashes. Un artefacto con hashes divergentes no se promueve. Cada release se firma bajo una política PQC y el nodo verifica firmas y manifest antes de instalarlo.

Fuzzing continuo, bug bounty, auditorías externas y adversarial testnets deben acompañar el desarrollo. “Self-healing” no es excusa para publicar software sin revisión; NeuroImmune es una capa adicional de resiliencia, no un sustituto de ingeniería segura.

PARTE VI

NEUROIMMUNE: RED AUTORREPARABLE Y ACTUALIZABLE

Aprender de incidentes, validar mitigaciones y desplegarlas sin detener el ledger.

NEUROCHAIN • Quantum Neural Blockchain

La idea central de NeuroImmune

Convertir un incidente local en inmunidad distribuida, con controles contra poisoning.

Figura 11. Ciclo de NeuroImmune desde la detección hasta el rollout.

El escenario de referencia es un nodo en Singapur que recibe un ataque desconocido. Su NeuroAgent detecta una anomalía, activa defensas locales permitidas y consigue mantener el nodo saludable. El nodo no envía un binario para que todos lo instalen; genera una Incident Capsule con huellas, evidencia, componente afectado, mitigación propuesta, tests y firmas.

Los demás validadores verifican la firma y reproducen el incidente en sandboxes. Diferentes implementaciones intentan confirmar que el problema existe y que la mitigación no rompe invariantes. Las attestations de reproducción se agregan como evidencia distribuida. Solo después de alcanzar la política de aprobación aplicable se crea un artefacto candidate.

El principal riesgo de un sistema adaptativo es el poisoning: un atacante podría intentar convencer a un nodo de que una “mitigación” maliciosa funciona y propagarla. Por eso ningún nodo, ningún NeuroAgent y ningún operador individual tiene poder para actualizar la red. La actualización exige reproducción independiente, artefactos reproducibles, firmas, aprobación protocolaria y rollout por etapas.

No todo incidente genera una nueva versión del binario. Muchas defensas pueden representarse como Security Policy Packs: límites, fingerprints, reglas P2P, listas temporales, modelos de detección

o configuraciones firmadas. Separar policy version de node version permite responder en segundos o minutos sin convertir cada anomalía en un fork.

Shadow mode, canary rollout y A/B runtime

Actualizar sin apostar el 100% de la red a una versión no probada.

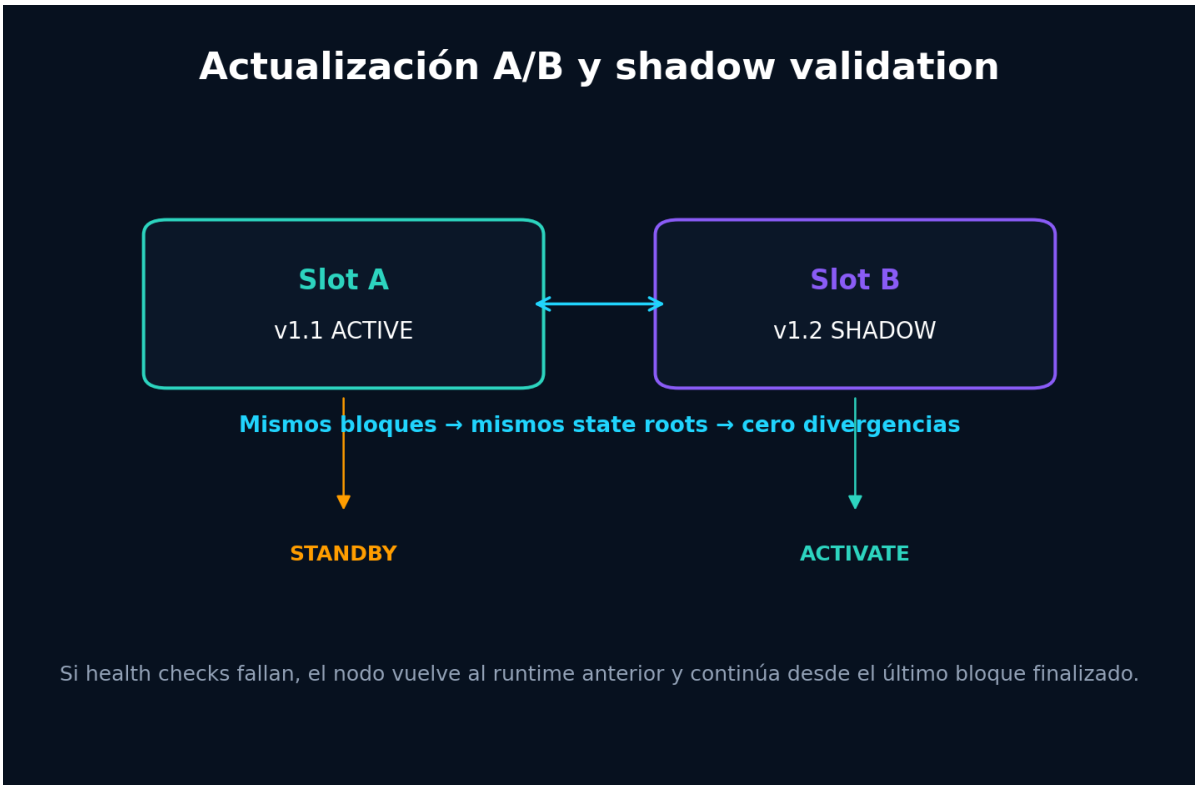

Figura 12. Un runtime activo puede convivir temporalmente con un runtime shadow.

El mecanismo de actualización debe mantener dos slots de runtime o una capacidad equivalente. La versión activa procesa consenso. La candidata recibe los mismos bloques en shadow mode, ejecuta la transición de estado y compara state roots sin tener autoridad para producir decisiones. Cero divergencias durante una ventana definida aumenta confianza antes de activar.

El rollout comienza con una cohorte canary pequeña y suficientemente diversa. Se comparan finality, memoria, CPU, errores, divergencias y comportamiento de networking. Si los health checks permanecen dentro de límites, el porcentaje aumenta por waves. Si se supera un threshold de error, el rollout se congela y los nodos actualizados regresan al slot previo.

El rollback es de software, no del ledger. Si v1.2 falla después de que Block N fue finalizado, el nodo vuelve a v1.1 y continúa desde Block N+1 utilizando el estado comprometido compatible. Cuando una migración de schema hace esto imposible, debe utilizarse dual-write, snapshots versionados o una ventana explícita de compatibilidad.

Taxonomía de incidentes y upgrades

No todos los problemas merecen el mismo mecanismo de respuesta.

Nivel	Ejemplo	Respuesta típica	Autorización
L0	Anomalía local	Mitigación local / alert	Node policy
L1	Spam o P2P abuse	Security Policy Pack	Policy quorum
L2	Bug de cliente	Hot patch / rolling update	Release quorum
L3	Bug de protocolo	Coordinated protocol upgrade	Governance + BFT
L4	Vulnerabilidad crítica	Emergency canary + accelerated rollout	Emergency multi-party rule
L5	Primitive criptográfica comprometida	Crypto-suite migration	Highest-assurance governance

Esta clasificación limita la tentación de activar procedimientos de emergencia por cualquier error. Los mecanismos más poderosos deben ser más difíciles de utilizar. Una mala configuración de un nodo no debe activar gobernanza global; una vulnerabilidad de consenso sí puede requerir una ruta de emergencia.

Cada incidente y upgrade genera un registro público de alto nivel en el explorer: identificador, versión afectada, tipo, estado, porcentaje de rollout y hashes de artefactos. Los detalles que facilitarían explotación pueden permanecer embargados hasta que la red esté protegida y el disclosure sea seguro.

Actualización sin downtime

Cómo preservar continuidad del servicio durante evolución de protocolo.

La coexistencia de versiones es una capacidad que debe diseñarse, no improvisarse. Durante una ventana de upgrade, v1.1 y v1.2 deben entender una parte común del protocolo. El activation epoch marca cuándo nuevas reglas se vuelven obligatorias. Los nodos rezagados pueden seguir sincronizando hasta el límite de compatibilidad y reciben alertas antes de quedar fuera del validator set.

Para cambios mayores, puede utilizarse feature gating: la nueva capacidad existe en el binario pero permanece inactiva hasta una condición de red. Esto permite distribuir software con anticipación, observar estabilidad y activar de manera coordinada sin reinicios masivos simultáneos.

Los clientes deben guardar manifests de estado, versión de DB y rutas de migración. Un nodo que no pueda completar una migración de forma segura debe entrar en modo no-validador antes que producir estado divergente. La disponibilidad se prioriza, pero nunca a costa de safety.

PARTE VII

NEUROAI: INTELIGENCIA NATIVA EN VALIDADORES

Agentes distribuidos que observan y atestiguan sin reemplazar consenso matemático.

NEUROCHAIN • Quantum Neural Blockchain

NeuroAgent: función, límites y autonomía

La IA dentro del nodo, no una API central que controle toda la red.

Cada NeuroValidator ejecuta un NeuroAgent local o un conjunto de modelos locales. El agente puede analizar transacciones, peers, contratos, comportamiento de red y telemetría. Debe operar aunque un proveedor externo no esté disponible; una dependencia obligatoria de una API central anularía parte de la descentralización.

La output principal es una attestation estructurada. Ejemplos de campos: tx hash, validator ID, model ID, policy version, decision class, risk score, confidence, reason codes, evidence hash y signature. Este formato permite auditar qué política estaba activa cuando se tomó una decisión sin exigir que todos compartan el mismo modelo.

La IA no decide unilateralmente si una firma válida es “propiedad legítima” ni puede confiscar fondos por una opinión. Las restricciones que utilicen AI risk —por ejemplo cuentas reguladas o bridges institucionales— deben estar declaradas en la política de la cuenta o aplicación. El protocolo base preserva reglas objetivas.

Los NeuroAgents también participan en seguridad operacional: detectan patrones de DoS, degradación, anomalías de peer, divergencias de software, posibles compromises y cambios de distribución. Sus alertas alimentan NeuroImmune, donde pasan por reproducción y reglas de autorización antes de producir cambios globales.

AI Attestations

Convertir análisis probabilístico en evidencia pequeña, firmada y consultable.

Campo conceptual	Propósito
tx_hash / event_hash	Vincular la attestation a un objeto exacto
validator_id	Identificar emisor
model_id	Saber qué modelo produjo el resultado
policy_id	Versionar criterios
risk_score	Señal cuantitativa
decision_class	ACCEPT / REVIEW / ALERT u otra taxonomía
reason_codes	Explicación estructurada
evidence_hash	Compromiso a evidencia extensa
pq_signature	Autenticidad de la attestation

La attestation debe ser suficientemente pequeña para no hinchar bloques. En escenarios de alto throughput puede agregarse por lote o almacenarse bajo estructuras que permitan proofs de inclusión. El diseño final equilibrará auditabilidad, bytes por TX y utilidad operativa.

Los modelos pueden evolucionar sin exigir fork. Model ID y policy ID forman parte de la attestation; el explorer permite comparar comportamiento por versión. Cambios que alteren semantics críticas sí requieren una policy upgrade autorizada.

Sistema inmunológico distribuido y aprendizaje

Compartir métodos de defensa sin compartir automáticamente código ejecutable.

La idea de “un nodo aprende y todos aprenden” se implementa mediante objetos verificables, no mediante confianza ciega. Un nodo transmite fingerprints, metadatos de mitigación y tests; la red reproduce. El conocimiento que se propaga puede ser una policy, una regla de detección o un candidate patch, cada uno con un nivel diferente de control.

Con el tiempo, la red puede mantener un corpus de incidentes: tipos de ataque, targets, eficacia de mitigaciones, regiones, versiones y falsos positivos. Parte de ese corpus puede ser público y parte restringido. Los NeuroAgents pueden entrenarse o ajustarse sobre datos agregados sin que información sensible de usuarios se vuelva pública.

Este mecanismo crea una memoria operacional distribuida. La ventaja competitiva no sería que NEUROCHAIN “nunca es atacada”, sino que intenta reducir el tiempo entre primera detección, contención, validación de defensa e inmunización del resto de la red.

PARTE VIII

NEUROISO Y FINANZAS

ISO 20022 como semántica financiera nativa, con privacidad y evidencia on-chain.

NEUROCHAIN • Quantum Neural Blockchain

ISO 20022: qué es y qué no es

Un estándar de mensajes, no una certificación mágica para una blockchain.

ISO 20022 define modelos y mensajes para la industria financiera. Sus catálogos incluyen familias como pain para iniciación de pagos, pacs para clearing/settlement y camt para cash management. Decir que una blockchain es “ISO 20022” no debería significar simplemente que guarda una referencia de texto; la integración debe mapear semántica, versionado, identidad, privacidad y settlement.

NeuroISO se plantea como una capa que entiende tipos de mensaje y puede vincular un evento financiero tradicional con una operación NEUROCHAIN. El mensaje completo puede permanecer cifrado fuera del ledger bajo controles institucionales; el ledger conserva hash, tipo, referencias, autorización, timestamps y settlement proof.

La red debe versionar packs ISO porque las definiciones evolucionan. Un mensaje pacs.008 de una versión no debe interpretarse implícitamente como otra. El hash se calcula sobre una representación canonicalizada definida, evitando que diferencias irrelevantes de serialización alteren la evidencia.

Figura 13. Flujo conceptual NeuroISO y separación entre privacidad y settlement.

Modelo de privacidad para datos financieros

Anclar evidencia sin publicar PII o mensajes bancarios completos.

Publicar información bancaria detallada en una blockchain pública sería incompatible con múltiples obligaciones de privacidad y con una arquitectura prudente. NeuroISO debe soportar referencias opacas, cifrado, permisos y selective disclosure. Las partes autorizadas pueden demostrar que un documento corresponde al hash comprometido sin revelar su contenido a toda la red.

El ledger puede conservar información mínima: familia de mensaje, message ID o reference hash, EndToEndId/UETR cuando la política lo permita, entidad autorizadora pseudonimizada, settlement asset, outcome y commitment. El resto vive en storage institucional o distribuido cifrado.

La arquitectura debe permitir que bancos o empresas usen gateways sin convertir esos gateways en validadores privilegiados. La función financiera y la función de consenso permanecen separadas: una entidad puede emitir/consumir mensajes ISO sin controlar el ledger.

Tokenización, pagos y activos institucionales

Unificar settlement nativo con referencias financieras verificables.

Una vez que NeuroISO, cuentas PQ y smart contracts conviven, NEUROCHAIN puede servir como rail para tokenización de activos, pagos institucionales, stable assets, RWA y workflows que necesitan rastrear referencias tradicionales. La fortaleza está en vincular el estado on-chain con una semántica conocida por sistemas financieros existentes.

El protocolo no debe imponer compliance global a todas las cuentas. En su lugar, módulos, contratos o cuentas institucionales pueden exigir KYC attestations, policies de autorización o AI review según su jurisdicción. Esto preserva una base permissionless mientras habilita zonas reguladas explícitas.

El diseño de activos, stablecoins y tokenización pertenece a capas superiores y requerirá análisis legal. Este dossier se limita a la infraestructura que permitiría transportar autorizaciones, referencias y settlement de forma verificable.

PARTE IX

INTEROPERABILIDAD, WALLETS Y DESARROLLADORES

Entrar en el ecosistema existente sin renunciar a cuentas nativas post-cuánticas.

NEUROCHAIN • Quantum Neural Blockchain

Compatibilidad de wallets

Interoperar por capas en lugar de degradar el núcleo.

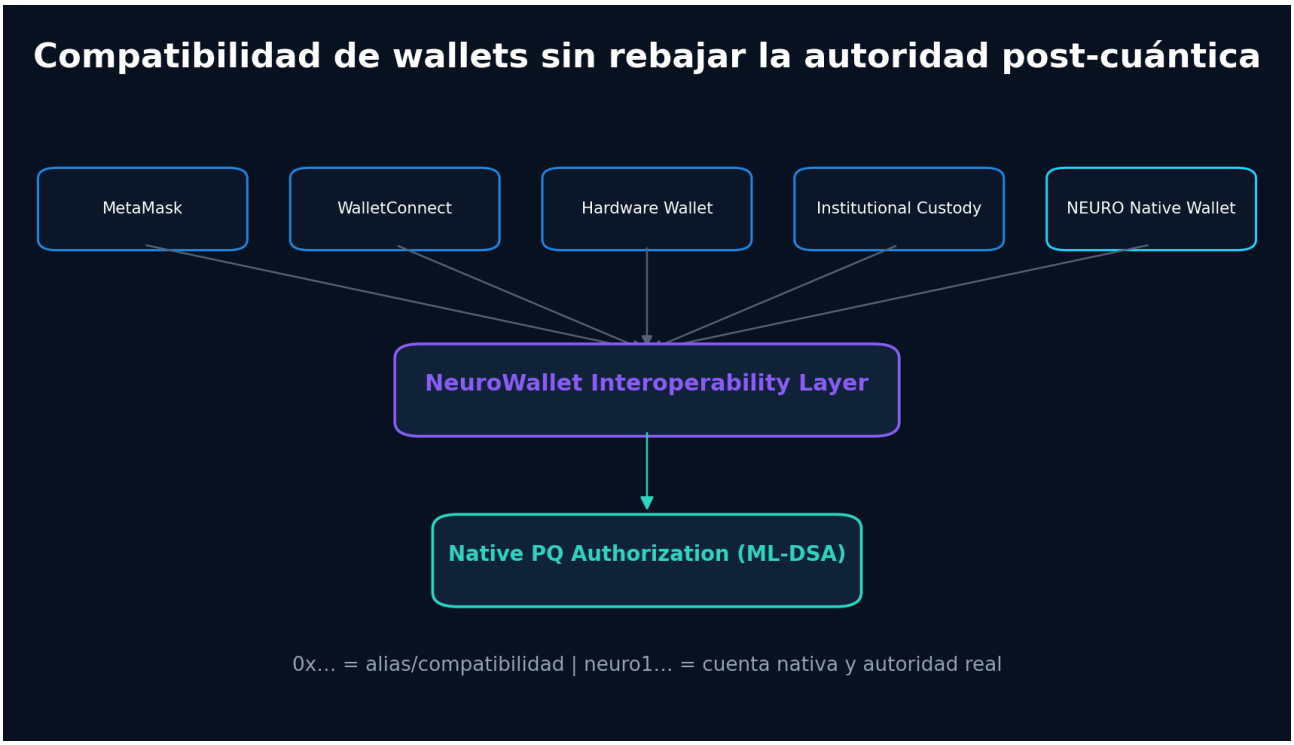

Figura 14. Wallet interoperability con autorización PQ nativa.

Una wallet existente que solo produce secp256k1 o Ed25519 no puede generar por sí sola una firma ML-DSA. La solución incorrecta sería permitir que la firma legacy sea suficiente para mover fondos nativos, porque se heredaría la superficie de seguridad que NEUROCHAIN pretende evitar.

La solución es un NeuroWallet Interoperability Layer. MetaMask, WalletConnect, custodios y hardware wallets pueden expresar identidad, intención o aliases. Un PQ signer nativo —en wallet, Snap, smart account, hardware o módulo institucional— produce la autorización final aceptada por la cuenta NEUROCHAIN.

WalletConnect es relevante por su diseño multichain y onboarding basado en CAIP. MetaMask Snaps puede ampliar protocolos y tipos de cuenta. Sin embargo, las capacidades exactas de cada wallet pueden cambiar; la compatibilidad se publica por versión y se valida contra APIs oficiales.

QRYPTA Wallet o una NeuroWallet de referencia puede convertirse en la experiencia nativa completa: generación de claves PQ, recovery, smart accounts, NeuroISO, NeuroAgent personal, staking y visualización de attestations. Las wallets externas conservan acceso mediante adapters.

Compatibilidad EVM sin convertirse en una EVM dependiente

RPC y herramientas como puente de adopción.

EVM compatibility puede reducir el coste de entrada para desarrolladores: namespaces JSON-RPC conocidos, herramientas de despliegue, Solidity o capas de ejecución compatibles. Pero la transacción EVM debe encapsularse en un envelope NEUROCHAIN que respete las reglas nativas de autorización, fees y state commitment.

El prefijo 0x puede aparecer en una vista de compatibilidad, mientras el explorer muestra siempre la identidad nativa vinculada. Un contrato o dApp puede usar APIs EVM sin obligar a que la cuenta de seguridad primaria sea ECDSA.

La meta no es replicar Ethereum bit a bit, sino ofrecer un conjunto de compatibilidad suficiente para migración y UX. Las capacidades que comprometan throughput, PQC o account abstraction deben implementarse mediante adaptadores, no incrustarse en el consenso principal.

SDK, APIs y experiencia del desarrollador

Una L1 avanzada debe seguir siendo simple para quien construye.

Superficie	Ejemplos conceptuales
RPC	status, block, tx, address, validators
WebSocket	new block, finalized tx, validator health
AI API	attestation lookup, risk aggregate
ISO API	message reference lookup, settlement proof
Wallet SDK	account creation, signing, session keys
EVM compatibility	selected eth_* methods / adapter
Indexer API	search, analytics, historical state

La complejidad interna de NeuroBFT, PQC o NeuroImmune no debe filtrarse a un desarrollador que solo quiere transferir un token. El SDK debe ofrecer defaults seguros y abstracciones de alto nivel, mientras los operadores avanzados conservan acceso a datos de protocolo.

Documentación, ejemplos, testnet faucet, local devnet y explorer son productos de primer nivel. Una gran arquitectura sin tooling produce una red técnicamente elegante pero vacía.

PARTE X

EXPLORER, OBSERVABILIDAD Y TRANSPARENCIA

Hacer visible no solo bloques y TX, sino PQC, IA, consenso, ISO y upgrades.

NEUROCHAIN • Quantum Neural Blockchain

NEUROCHAIN Explorer

El portal público de evidencia y salud de red.

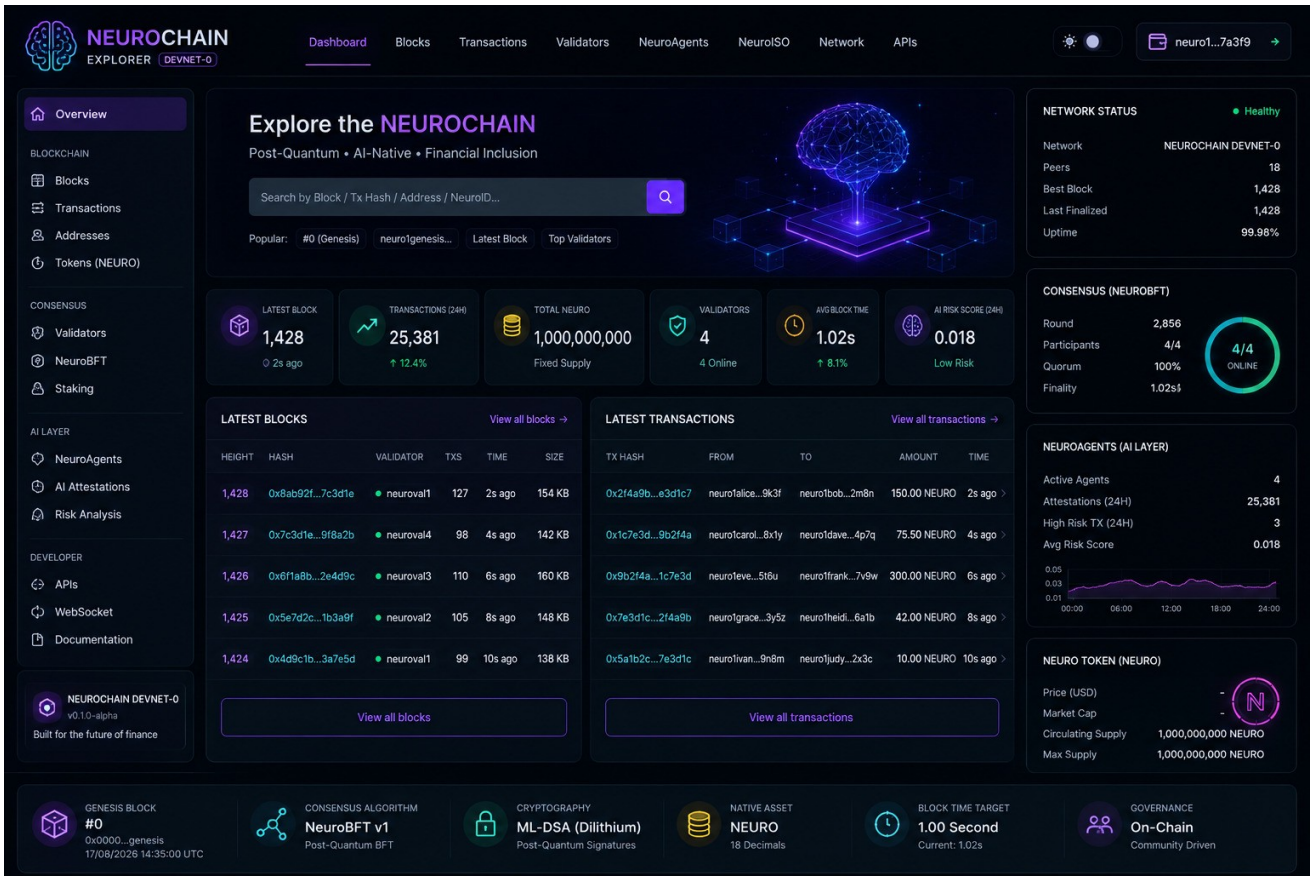

Figura 15. Mockup conceptual del NEUROCHAIN Explorer desarrollado durante la fase de diseño.

El explorer no debe consultar directamente a validadores en cada vista. Los nodos emiten eventos hacia indexadores, los indexadores escriben bases de datos optimizadas y un API cluster sirve a web, wallet y dashboards institucionales. Esta separación permite escalar el explorer horizontalmente sin afectar consenso.

Además de bloques, transacciones, direcciones y tokens, el explorer puede exponer validators, NeuroAgents, AI attestations, risk aggregates, NeuroBFT rounds, crypto suite, ISO references, software versions y el historial de upgrades. La transparencia convierte capacidades abstractas en evidencia que inversores, desarrolladores y auditores pueden comprobar.

A 200K SFTPS, la UI no intentará mostrar cientos de miles de filas por segundo. Presentará agregados en tiempo real y recuperará objetos individuales bajo demanda. WebSockets pueden actualizar latest block, finality, validator health y TPS sin recargar la página.

Figura complementaria. Arquitectura de indexación y API del explorer a escala.

Métricas de red y panel de seguridad

Medir salud antes de que el usuario note una degradación.

- Current / sustained SFTPS y composition de carga.
- Finality p50, p95 y p99 por región.
- Número de validadores activos, effective stake y concentración.
- Client diversity, cloud diversity y geographic diversity.
- PQC verification latency y bytes por firma/transacción.
- NeuroAgent fast-path latency y porcentaje de deep-path.
- Incidentes NeuroImmune abiertos, rollout waves y rollback count.
- Version adoption del node client, consensus, crypto suite, AI policy e ISO pack.
- State growth, snapshot size y sync time.
- Peer health, retransmisiones y bandwidth saturation.

Estas métricas deben alimentar alertas y reportes públicos sin exponer información que facilite ataques. El nivel público y el nivel SOC/validator pueden tener granularidades distintas.

PARTE XI

MVP, LABORATORIO Y TESTNET

Cómo pasar de una sola PC al primer entorno público distribuido.

NEUROCHAIN • Quantum Neural Blockchain

NEUROCHAIN LAB-01

La workstation de desarrollo como primer laboratorio reproducible.

Componente de referencia	Configuración planificada
CPU	Intel Core i7-13700F
RAM	64 GB DDR4
GPU	NVIDIA GeForce RTX 5070 12 GB
Storage	1 TB NVMe PCIe 4.0
Motherboard	ASUS PRIME B760M-P D4
Cooling	Cooler Master 240 mm AIO
PSU	850 W 80+ Gold
Uso	4 validators locales + AI + explorer + benchmark

Esta workstation es adecuada para DEVNET-0, compilación, inferencia local y pruebas funcionales. No representa el benchmark final de mainnet. Cuatro procesos independientes pueden simular el validator set local, cada uno con puertos, state DB, claves y NeuroAgent separados.

La primera fase valida hardware y software base: BIOS, memoria, NVMe, temperaturas, GPU, drivers, Linux y estabilidad bajo CPU+GPU. Después se crea la toolchain, el repositorio y el cliente inicial. El objetivo es que el MVP sea la semilla del código real y no una demo desechable.

Block #0 y los primeros días

Genesis como evidencia técnica, no como animación.

1. Día 1: validar workstation, instalar entorno, repo, compilación y base del cliente.
2. Día 2: cuentas PQ, direcciones neuro1..., formato de transacción, firmas y verificación.
3. Días 2–4: genesis.json, state inicial, Block #0, hash y release firmada.
4. Días 3–5: primeras transferencias, Block #1/#2, RPC y logs reproducibles.
5. Semana 1–2: cuatro nodos, networking y primera versión de NeuroBFT.
6. Semanas 2–3: NeuroAgents y AI attestations.
7. Semanas 3–4: NeuroISO, explorer y faucet.
8. Semanas 4–6: DEVNET-0 integrada, fault testing y benchmarks iniciales.

Genesis — El hash de Block #0, el genesis file y el commit que lo genera deben preservarse y publicarse cuando corresponda. A partir de ese momento la red tiene una historia verificable.

Evolución hacia una testnet pública

Separar físicamente validadores para medir la red real.

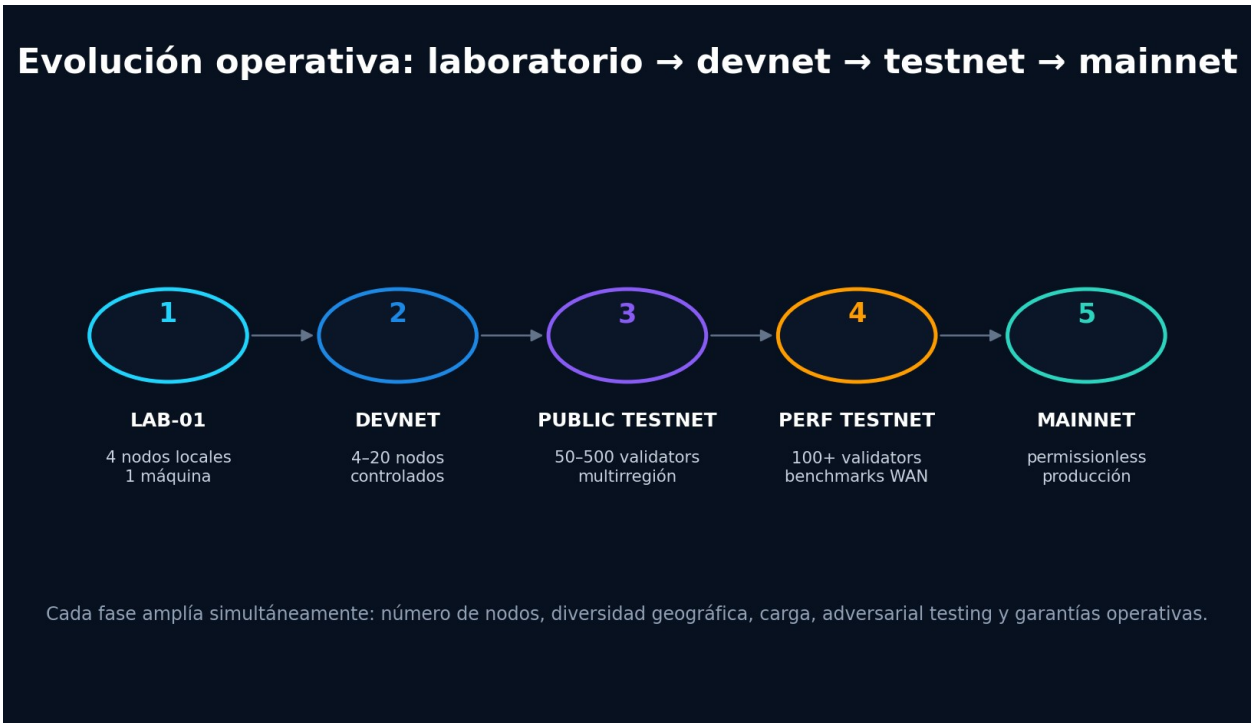

Figura 16. Fases de despliegue desde LAB-01 hasta mainnet.

Después de demostrar cuatro nodos locales, el siguiente salto no es aumentar TPS en localhost, sino separar los nodos: América, Europa, Asia y otra región. Esto introduce latencia WAN, jitter, pérdida de paquetes, diferentes proveedores y sincronización real.

La testnet pública puede crecer de 20 a 50, 100 y 500 validadores. El faucet entrega tNEURO sin valor; los operadores prueban el flujo de registro, stake, activación, key rotation, upgrade y salida. La red recopila datos para diseñar requisitos mínimos y economía de mainnet.

El programa de validadores debe buscar diversidad deliberada: universidades, empresas, comunidad, datacenters, nodos domésticos y distintos países. La descentralización no surge automáticamente al abrir un formulario; debe medirse y cultivarse.

Adversarial testnet

Atacar la red antes de pedir que el mercado confíe en ella.

- Apagar un validador durante consenso y medir continuidad.
- Simular double-sign, conflicting votes y mensajes malformados.
- Enviar firmas PQ inválidas a gran volumen.
- Spam de cuentas nuevas y replay de nonces.
- Faults de storage, disco lleno, snapshot corrupto y restart loop.
- Divergencia intencional de un cliente y detección por state roots.
- Ataques P2P de conexión, peer exhaustion y paquetes duplicados.
- NeuroAgent poisoning simulations.
- Upgrade candidate defectuoso y rollback A/B.
- Cambio simulado de crypto suite y rotación de claves.
- Carga ISO con referencias privadas y selective disclosure.
- Stress sostenido con composición realista, no solo transferencias triviales.

Los resultados deben publicarse con metodología y límites. Una falla detectada en testnet es un activo de ingeniería si se corrige y documenta; ocultarla reduce la capacidad de la red para demostrar madurez.

PARTE XII

POSICIONAMIENTO GLOBAL Y COMPETENCIA

Dónde podría ubicarse NEUROCHAIN si ejecuta el diseño y qué sigue faltando para competir con redes consolidadas.

NEUROCHAIN • Quantum Neural Blockchain

Comparación conceptual con generaciones existentes

Tecnología integrada versus efecto de red.

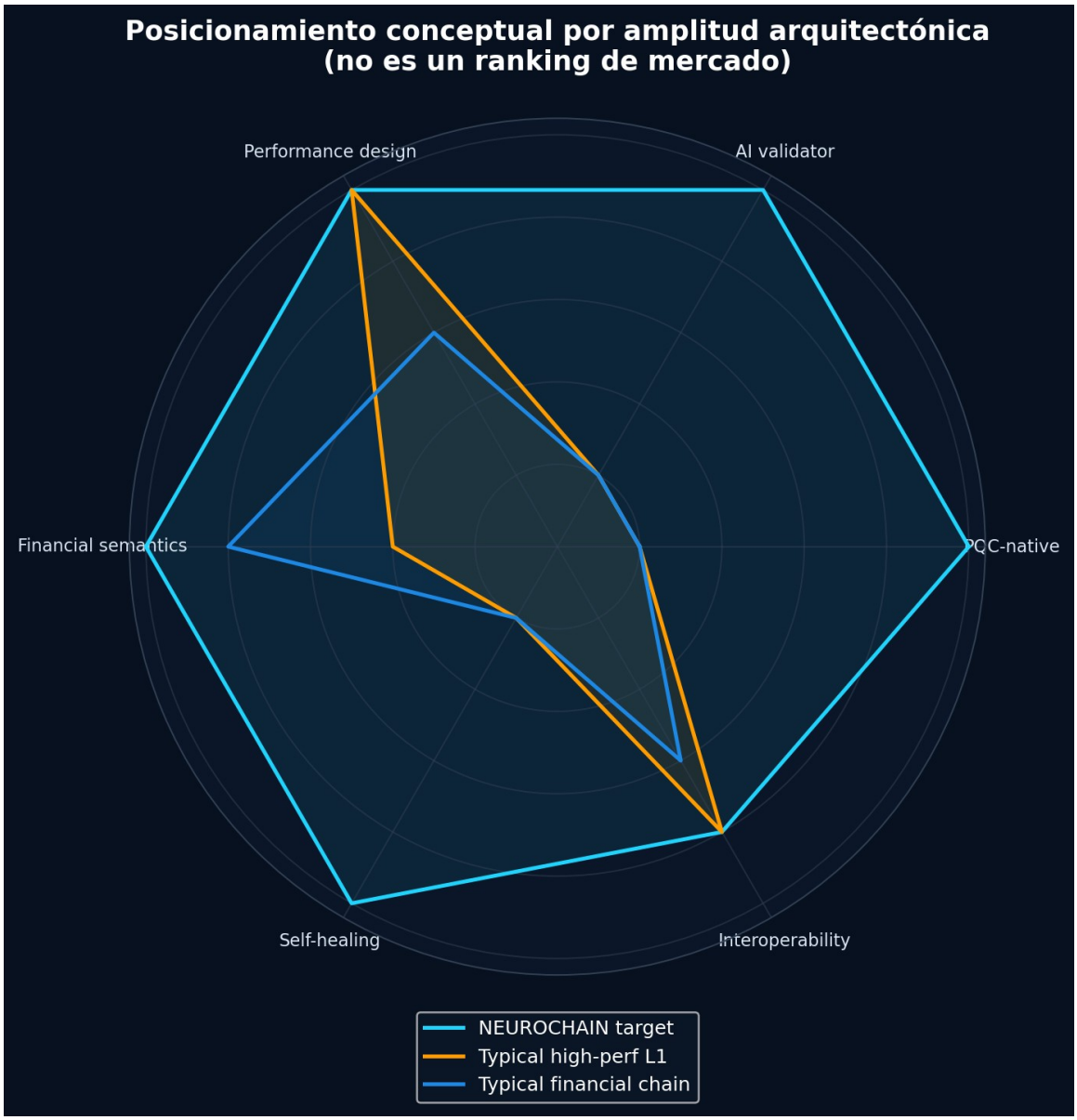

Figura 17. Posicionamiento conceptual por amplitud arquitectónica; no es un ranking económico.

Ethereum representa una referencia en programmability, ecosistema y client diversity; además trabaja en evolución de seguridad y transición post-cuántica. XRPL es una referencia en pagos, finality y longevidad operacional. Solana demuestra el valor de ejecución paralela y pipeline de alto rendimiento. Sui publica benchmarks de Mysticeti cercanos a 200K TPS con baja latency. Estas redes establecen el nivel de evidencia que NEUROCHAIN deberá superar en diferentes dimensiones.

La oportunidad de NEUROCHAIN reside en la combinación: PQC desde Genesis, AI agents dentro de validadores, ISO 20022 protocol-native, NeuroImmune, crypto-agility, execution parallelism y un objetivo de high-performance permissionless consensus. Ninguna de estas palabras por separado es suficiente; la diferenciación aparece si todas funcionan simultáneamente bajo tests públicos.

El día de Genesis, NEUROCHAIN será un proyecto nuevo sin el historial, liquidez, apps, usuarios ni años de battle testing de ETH, XRPL o Solana. Una arquitectura superior en papel no equivale a una posición de mercado. El posicionamiento técnico se gana con testnet y auditorías; el posicionamiento económico se gana con desarrolladores, activos, wallets, instituciones y comunidad.

Referencias públicas actuales

Red / estándar	Referencia relevante para NEUROCHAIN
Ethereum	Proof of Stake, client diversity y roadmap de seguridad/PQC
XRPL	Consensus con finality, pagos y sistema de amendments
Solana	Sealevel y ejecución paralela / data pipeline
Sui	Mysticeti y benchmark oficial cercano a 200K TPS
NIST	FIPS 203/204/205 para ML-KEM, ML-DSA y SLH-DSA
ISO 20022	Catálogo formal de mensajes y mantenimiento de schemas
WalletConnect	Onboarding multichain mediante CAIP-25
MetaMask Snaps	Extensión de protocolos y tipos de cuenta

Qué tendría que demostrar para ser una L1 de primera línea

La lista que separa una promesa de una infraestructura global.

- Testnet pública con cientos de validadores independientes y diversidad geográfica.
- PQC end-to-end medible: cuenta, validador, block/attestation, networking y software supply chain.
- NeuroBFT con especificación pública, model checking y comportamiento BFT validado.
- Benchmarks WAN reproducibles acercándose progresivamente a 200K SFTPS.
- NeuroImmune demostrado en incident simulations con canary, shadow mode y rollback.
- NeuroISO con privacy model, versionado de messages y casos institucionales reales.
- Al menos dos clientes independientes antes de madurez de mainnet.
- Auditorías de protocolo, criptografía, smart contract/runtime y operación.
- Wallet interoperability sin downgrade de autorización nativa.
- Ecosistema: SDKs, stable assets, DEX, bridge, custodios, developers y partners.

PARTE XIII

ECONOMÍA, PRESUPUESTO Y RUTA A MERCADO

Capital escalonado por evidencia: invertir más solo cuando la fase anterior demuestra valor.

NEUROCHAIN • Quantum Neural Blockchain

Rangos de inversión

De laboratorio de miles de dólares a mainnet de varios millones.

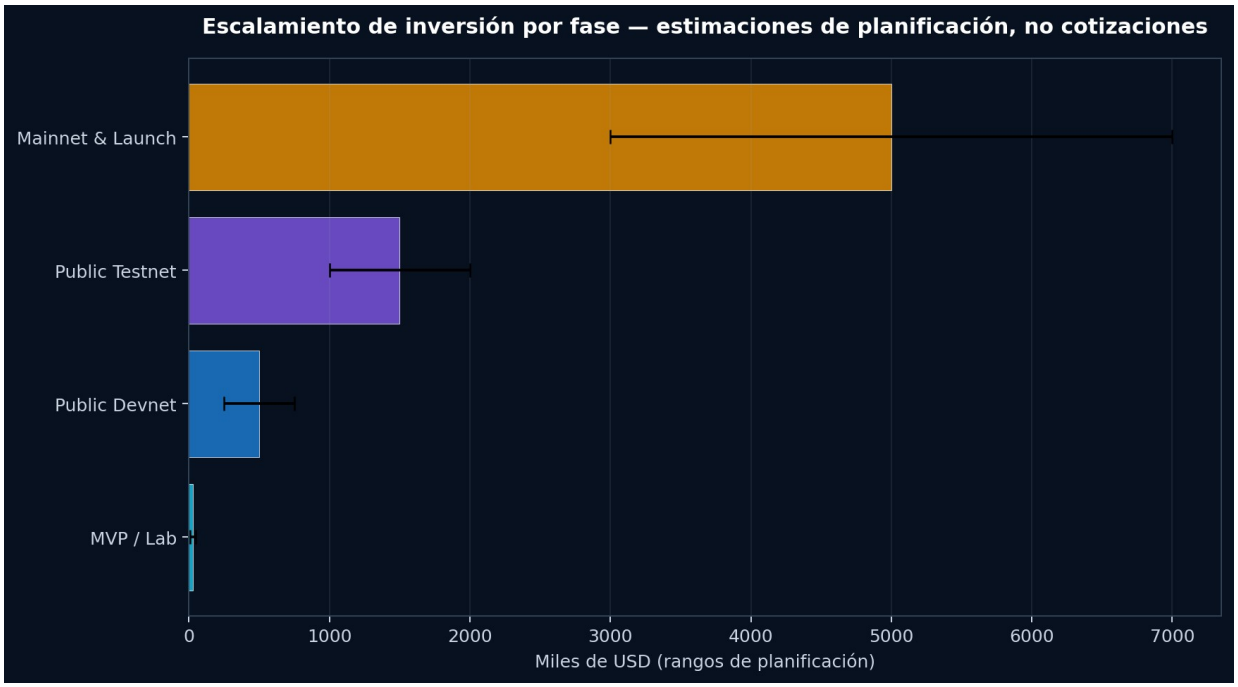

Figura 18. Rangos de planificación financiera discutidos para cada fase.

Fase	Rango orientativo	Objetivo
MVP / LAB	USD 10K–50K	Genesis, PQ accounts, 4 nodes, explorer base
Public Devnet	USD 250K–750K	20+ nodes, wallet integrations, SDK, EVM adapter
Public Testnet	USD 1M–2M adicional	50–500 validators, audits, staking, WAN load
Mainnet & Launch	USD 3M–7M adicional	Production infra, multi-client, formal verification, institutional integrations

Estos rangos son estimaciones de planificación, no cotizaciones. La cifra real depende del tamaño del equipo, país, contratación, auditorías, infra, scope de VM, acuerdos de wallet y velocidad de ejecución. Para una mainnet comercial seria, el rango acumulado discutido es aproximadamente USD 5–10M; un lanzamiento institucional de máxima ambición puede requerir USD 10–15M o más.

El principio financiero es milestone-based funding. No se levanta todo el capital para probar si Block #0 funciona. El laboratorio demuestra el núcleo; la devnet demuestra distribución; la testnet demuestra adversarial resilience; auditorías y benchmarks abren el capital de mainnet.

Equipo mínimo por disciplina

Qué capacidades humanas se necesitan conforme crece la red.

Disciplina	Responsabilidad
Protocol / distributed systems	Consensus, networking, data plane, state
Cryptography / PQC	Suites, key management, migration, audits
Runtime / VM	Parallel execution, contracts, determinism
AI / security ML	NeuroAgents, anomaly models, attestations
Security engineering	Threat model, fuzzing, incident response, NeuroImmune
DevOps / SRE	Release, observability, multi-region testnet
Wallet / SDK	Native accounts, WalletConnect, adapters
Financial messaging	ISO 20022 mapping and privacy
Frontend / Explorer	Explorer, dashboards, developer UX
Formal methods / audit	Safety invariants and independent verification

No todas estas funciones necesitan ser equipos grandes en el MVP. La prioridad inicial es protocol engineering, PQC, networking, test harness y una implementación simple del NeuroAgent. El resto crece al pasar a public testnet.

Go-to-market técnico

La tecnología debe ser demostrable antes de convertirse en narrativa comercial.

1. Publicar arquitectura de alto nivel y límites de claims.
2. Mostrar Genesis y transacciones PQ reales en explorer.
3. Abrir DEVNET con documentación para operadores externos.
4. Publicar benchmark methodology y resultados reproducibles.
5. Lanzar validator program y dashboard de descentralización.
6. Abrir SDK, wallet integrations y EVM compatibility.
7. Demostrar NeuroImmune en una prueba pública controlada.
8. Publicar auditorías y roadmap de remediation.
9. Incorporar partners de pagos, RWA, custody y stable assets.
10. Mainnet Genesis solo cuando las condiciones de seguridad y operación estén satisfechas.

PARTE XIV

GOBERNANZA, RIESGOS Y CRITERIOS DE ÉXITO

Cómo impedir que las capacidades de emergencia o IA se conviertan en fuentes de centralización.

NEUROCHAIN • Quantum Neural Blockchain

Gobernanza de protocolo y emergencia

Poderes específicos, auditables y limitados.

Una red actualizable necesita gobernanza, pero una gobernanza excesivamente poderosa puede convertirse en backdoor. Las capacidades se separan: activar una security policy no es lo mismo que cambiar una regla de supply o migrar una suite criptográfica. Cada clase utiliza quorums, delays y procedimientos proporcionales al riesgo.

La gobernanza de emergencia puede acelerar un rollout cuando una vulnerabilidad activa amenaza la red, pero no debe permitir editar balances arbitrariamente. Las emergency actions se definen por alcance y expiración, generan eventos públicos y pasan a post-mortem obligatorio.

La participación de validadores y stakeholders debe evitar plutocracia pura. Delegación, caps de stake, reputación operativa y límites de concentración pueden estudiarse, pero cualquier mecanismo adicional debe conservar verificabilidad y evitar que una entidad cree identidades ilimitadas para esquivar caps.

Registro de riesgos

Los riesgos principales deben existir por escrito antes de convertirse en incidentes.

Riesgo	Severidad	Mitigación de arquitectura
Complejidad excesiva	Alta	Diseño modular, interfaces pequeñas, feature gating, milestones
Overhead PQC	Alta	Batching, caches, formatos compactos, hardware benchmarks
IA introduce latencia	Alta	Fast/deep path, async analysis, compact attestations
PoS concentration	Alta	Effective stake caps, dashboards, validator diversity
Update poisoning	Crítica	Reproduction, reproducible builds, quorum, canary, rollback
Client monoculture	Alta	Segunda implementación independiente
State growth	Alta	Archival roles, snapshots, pruning policies
ISO privacy leak	Crítica	Encryption, minimization, selective disclosure
Wallet downgrade	Alta	Legacy alias ≠native authorization
200K claim no alcanzado	Media	Public methodology; optimize iteratively; no false claims
Regulatory uncertainty	Media/Alta	Modular institutional policies, counsel by jurisdiction
Supply chain compromise	Crítica	Signed manifests, multiple builders, isolated release pipeline

Criterios de éxito por fase

Qué debe estar comprobado antes de avanzar.

Fase	Go / No-Go mínimo
LAB-01	PQC accounts + Genesis + deterministic state + stable hardware
DEVNET-0	4-node BFT + AI attestations + fault recovery + explorer
WAN DEVNET	Multi-region finality + upgrade test + network profiling
PUBLIC TESTNET	Validator onboarding + staking + wallets + audits in progress
PERF TESTNET	Sustained load, adversarial test, crypto migration drill, multiple clients
MAINNET	Audits remediated, governance live, incident playbooks, economic security, ecosystem readiness

Ninguna fase debe saltarse porque una demo visual sea convincente. Los criterios de seguridad y reproducibilidad tienen prioridad sobre una fecha comercial.

KPIs estratégicos de NEUROCHAIN

Medir una arquitectura multiobjetivo sin reducirla a TPS.

Dimensión	Indicadores
Performance	SFTPS, finality p99, bytes/TX
Security	critical findings open, incident MTTD/MTTR, rollback success
PQC	verification latency, suite adoption, migration drill time
Decentralization	Nakamoto-like concentration measures, regions, clouds, clients
AI	fast-path latency, attestation rate, false positive rate
Availability	network uptime, validator participation, sync recovery
Ecosystem	active developers, wallets, contracts, assets
Financial	ISO message integrations, institutional pilots
Upgradeability	version adoption time, shadow divergence count
Transparency	public dashboards, reproducible benchmark coverage

PARTE XV

APÉNDICES

Glosario, ejemplos no secretos, checklist y fuentes de referencia.

NEUROCHAIN • Quantum Neural Blockchain

Apéndice A — Glosario

Término	Definición
AI Attestation	Objeto firmado que resume el análisis de un NeuroAgent sobre una TX/evento.
Crypto-agility	Capacidad de reemplazar algoritmos y suites sin destruir la continuidad del sistema.
Effective stake	Stake que realmente pesa en consenso después de caps o reglas de concentración.
Finality	Punto a partir del cual el protocolo considera una decisión irreversible bajo sus supuestos.
Hot path	Trabajo sincrónico que determina la latencia de una transacción.
ML-DSA	Esquema de firma post-cuántica estandarizado en FIPS 204.
ML-KEM	Mecanismo de encapsulación de claves post-cuántico estandarizado en FIPS 203.
NeuroBFT	Nombre conceptual del protocolo BFT de finalidad de NEUROCHAIN.
NeuroDAG	Data plane conceptual para diseminación paralela de batches.
NeuroImmune	Sistema de incident learning, validación y rollout seguro.
NeuroISO	Capa de mensajería financiera y settlement referenciado ISO 20022.
NeuroPoS	Mecanismo de admisión económica / validator set.
NeuroShield	Arquitectura de seguridad, PQC y crypto-agility.
NeuroVM	Runtime/ejecución paralela.
PQC	Post-Quantum Cryptography.
Shadow mode	Ejecución de una versión candidata sin autoridad de consenso para comparar resultados.
SLH-DSA	Firma post-cuántica basada en hashes estandarizada en FIPS 205.
SFTPS	Secure Finalized Transactions Per Second.
Validator committee	Subconjunto seleccionado para participar en una ronda/epoch.
Versioned state	Estado y schema que conservan compatibilidad y migración explícita entre versiones.

Apéndice B — Objetos públicos de ejemplo

Ejemplos ilustrativos; no representan formatos binarios ni schemas finales.

Cuenta nativa

neuro1q8v7w3m9k6t2x4p5s7c8d0n2h4j6l8f3a5z7q9

Validator ID

neuroval1k9d8m2x6p3s7z0q4n5t8c1h9j2f6w4r7y0e3

AI Attestation — campos visibles

Campo	Ejemplo
tx_hash	ntx1d9f3…7bc2
validator	neuroval1…
model	NeuroValidator-v0.1
policy	NAP-001
decision	ACCEPT
risk_score	0.018
confidence	0.991
evidence_hash	hash(…)
signature_scheme	ML-DSA

NeuroISO public commitment

Campo	Ejemplo
family	pacs.008
business_ref	opaque/reference
message_hash	hash(canonical message)
settlement_tx	ntx1…
privacy	encrypted external payload
authorization	PQ signed

No-implementation disclosure — No se incluyen layouts binarios, canonicalization algorithm final, IDs de fields internos, hashing domain separation, committee seed derivation ni parámetros de consenso.

Apéndice C — Checklist de DEVNET-0

La primera definición de “funciona”.

- ☐ Workstation validada bajo carga CPU+GPU.
- ☐ Repository y release process reproducible.
- ☐ 4 validators con states y claves independientes.
- ☐ Genesis file y Block #0 reproducibles.
- ☐ Cuentas neuro1… con firma PQ real.
- ☐ Transferencias y nonces deterministas.
- ☐ NeuroBFT produce bloques con 4/4 y continúa bajo fault permitido.
- ☐ NeuroAgent fast path activo.
- ☐ AI attestations firmadas y consultables.
- ☐ NeuroISO object de prueba.
- ☐ RPC y explorer conectados a datos reales.
- ☐ Nodo cae y resync sin corrupción.
- ☐ Upgrade candidate ejecutado en shadow mode.
- ☐ Rollback de software probado.
- ☐ Invalid signature / replay / spam tests.
- ☐ Benchmark generator y métricas exportadas.

Apéndice D — Checklist de testnet pública

Antes de invitar a operadores externos.

- ☐ Documentación de instalación y requisitos mínimos.
- ☐ Faucet tNEURO y validator onboarding.
- ☐ Public status page y explorer.
- ☐ Política de disclosure y bug bounty.
- ☐ Incident response playbook.
- ☐ Release signing y reproducible build evidence.
- ☐ Multi-region seed infrastructure sin dependencia central única.
- ☐ Dashboard de concentración de stake y diversidad.
- ☐ Upgrade / rollback drill público.
- ☐ Crypto-suite migration drill.
- ☐ WalletConnect / wallet adapter testado.
- ☐ ISO privacy review.
- ☐ External protocol/security audit iniciada.
- ☐ Backup/snapshot/restore procedures.
- ☐ SLA no prometido hasta recopilar datos.

Apéndice E — Fuentes técnicas de referencia

Fuentes primarias consultadas para estándares y comparación de patrones.

Ref.	Fuente
R01	NIST FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), final 2024.
R02	NIST FIPS 204 — Module-Lattice-Based Digital Signature Standard (ML-DSA), final 2024.
R03	NIST FIPS 205 — Stateless Hash-Based Digital Signature Standard (SLH-DSA), final 2024.
R04	ISO 20022 — Message Definitions Catalogue and maintenance materials.
R05	Ethereum.org — Proof of Stake, client diversity and security/post-quantum roadmap materials, consulted Aug 2026.
R06	XRPL.org — consensus protocol, finality, payments and amendments documentation, consulted Aug 2026.
R07	Solana documentation / architecture materials — Sealevel and parallel execution concepts.
R08	Sui Documentation — Mysticeti consensus; official benchmark description near 0.5s commit and 200K TPS, consulted Aug 2026.
R09	WalletConnect documentation — multichain onboarding with CAIP-25, consulted Aug 2026.
R10	MetaMask developer documentation — Snaps and custom account/protocol extension capabilities, consulted Aug 2026.
R11	HotStuff: BFT Consensus with Linearity and Responsiveness (research paper).
R12	Narwhal and Tusk / DAG-based BFT research family as architectural references for data dissemination and ordering separation.
R13	Hardware reference: Proforma #375752, 17 Aug 2026 — NEUROCHAIN LAB-01 planned workstation configuration.

Las fuentes competitivas se utilizan como referencia de patrones y benchmarks publicados por sus respectivos proyectos; no implican que sus métricas sean directamente comparables con NEUROCHAIN. Cualquier claim comercial futuro deberá acompañarse de metodología equivalente y fecha de consulta.

Apéndice F — Claims públicos y nivel de evidencia

Qué puede decirse en cada etapa sin confundir objetivo, benchmark y capacidad productiva.

Claim	DEVNET local	Public testnet	Mainnet madura
PQC-native	Demostrar firmas reales	Auditoría + networking PQ	Rotación y migration drills
AI-native validators	4 NeuroAgents locales	Operadores externos y modelos diversos	Métricas de producción y governance
High performance	Benchmark local contextualizado	SFTPS WAN reproducibles	Capacidad sostenida con carga real
Decentralized	No claim	Distribución de validators/stake	Diversidad sostenida y multi-client
ISO 20022 native	Schema/demo	Pilot institucional	Casos reales con privacy controls
Self-healing	Simulación controlada	Public incident drill	Historial de upgrades/rollback

La comunicación institucional debe avanzar al mismo ritmo que la evidencia. El claim más fuerte siempre debe apuntar a una prueba pública o a un artefacto auditable.

Apéndice G — Decisiones abiertas para la especificación v0.1

Preguntas que deben resolverse con prototipos, model checking y benchmarks; no por intuición.

- Parámetros exactos de ML-DSA por tipo de clave y lifetime.
- Formato final de cuenta neuro1… y domain separation de firmas.
- Diseño concreto de NeuroBFT y método de committee selection.
- Tamaño y cadencia de epochs, activación y unbonding.
- Modelo de effective stake cap y resistencia a entity splitting.
- Mecanismo de batch verification PQC y límites de TX size.
- Runtime de smart contracts y nivel de EVM compatibility.
- Conflict declaration / detection de NeuroVM.
- Persistencia de AI attestations: per-TX, batch o proof structure.
- Canonicalization y privacy profiles de NeuroISO.
- Condiciones exactas de canary promotion y automatic rollback.
- Requisitos mínimos de validator hardware derivados de testnet.
- Segunda implementación de cliente y lenguaje elegido.
- Metodología oficial de SFTPS y dataset de cargas reproducibles.

Regla — Estas decisiones permanecen deliberadamente abiertas hasta que exista evidencia suficiente. El dossier define el marco; la especificación de protocolo fijará los parámetros.

Conclusión

La ambición no es "tener muchas funciones"; es demostrar que pueden coexistir sin anularse.

NEUROCHAIN se plantea como una infraestructura de nueva generación: una Layer 1 permissionless cuyo diseño incorpora desde Genesis seguridad post-cuántica, agentes de IA locales dentro de validadores, finalidad BFT, paralelismo, semántica financiera ISO 20022, interoperabilidad con wallets y una arquitectura de actualización/rollback que intenta convertir incidentes aislados en aprendizaje distribuido.

La parte más difícil no será programar cada módulo individual. El reto verdadero es conservar simultáneamente safety, liveness, throughput, descentralización y operabilidad. Por eso el desarrollo debe avanzar mediante milestones medibles, con un hot path austero, interfaces versionadas, testnets adversariales y claims condicionados a evidencia pública.

El objetivo de 200.000 SFTPS debe funcionar como brújula de ingeniería y no como promesa prematura. Si la red demuestra rendimiento sostenido con PQC activa, IA nativa, cientos de validadores distribuidos y finality rápida, el resultado será mucho más significativo que un benchmark de transferencias en una sola máquina.

La seguridad a cien años no depende de adivinar hoy el algoritmo perfecto. Depende de construir una red que sepa cambiar de algoritmos, clientes, policies y hardware sin perder su ledger; que detecte fallos; que valide defensas de forma distribuida; y que pueda retroceder de software defectuoso sin reescribir su historia.

El siguiente hito es concreto: NEUROCHAIN LAB-01, Genesis Block #0, cuentas post-cuánticas y cuatro validadores locales. A partir de ahí, la visión deja de ser un documento y comienza a convertirse en evidencia ejecutable.

NEUROCHAIN

Quantum Neural Blockchain

PQC • AI-Native • High Performance • Decentralized • ISO 20022 • Self-Evolving