PROVIDENT
QUANTUM TECH

LIBRO BLANCO · EDICIÓN 2026 · v3.0

QRYPTA® Infraestructura financiera post-cuántica.

De dónde venimos, lo que construimos, dónde estamos y hacia dónde vamos. El token QRYP, la QRYPTA Wallet, el staking on-chain y la Layer 1 NEUROCHAIN, documentados para inversores, auditores, instituciones y desarrolladores.

EMISOR
Provident Quantum Tech S.R.L.

TOKEN
QRYP · BEP-20 · BNB Chain

FECHA
Septiembre 2026 · San José, CR

ÍNDICE

Contenido

SOBRE ESTE DOCUMENTO

Este Libro Blanco sustituye a la edición ejecutiva de abril de 2026. Describe el estado real y verificable del ecosistema QRYPTA® a septiembre de 2026 y el plan de desarrollo hacia NEUROCHAIN. Toda cifra on-chain citada puede comprobarse en las direcciones oficiales del Anexo A.

El documento no constituye oferta de valores, asesoría financiera ni promesa de rendimiento. La adquisición de activos digitales implica riesgos, descritos en el Capítulo 10.

Título	Libro Blanco QRYPTA® · Infraestructura financiera post-cuántica
Versión	3.0 · Septiembre 2026
Idioma	Español (edición en inglés disponible)
Emisor	Provident Quantum Tech S.R.L. · Cédula jurídica 3-102-965820 · Costa Rica
Marca	QRYPTA® · Registro Nº 419244 · Clases 9, 36 y 42 · vigente hasta 2036
Web	providentquantum.tech
Contacto	contact@providentquantum.tech · contact@qryptalabs.com

CAPÍTULO 01

Resumen ejecutivo

QRYPTA® es la primera infraestructura de transferencia de valor con criptografía post-cuántica en producción sobre redes EVM, y QRYP es el token que la coordina. Nacido en Costa Rica, el proyecto ya opera en BNB Chain con un contrato auditado por CertiK, staking no custodial y una wallet multichain, y avanza hacia una Layer 1 propia: NEUROCHAIN.

La computación cuántica amenaza la criptografía de curva elíptica (ECDSA / secp256k1) sobre la que descansan prácticamente todas las blockchains actuales. El NIST publicó en agosto de 2024 los tres primeros estándares post-cuánticos (FIPS 203, 204 y 205) y ha trazado la deprecación de los esquemas clásicos entre 2030 y 2035. La mayoría de la industria todavía discute cómo migrar. QRYPTA® resolvió la pregunta de forma práctica: la autoridad post-cuántica se ejerce **hoy**, sobre las redes que ya tienen liquidez, sin obligar a nadie a abandonar la EVM.

El mecanismo es simple de enunciar y difícil de ejecutar: cada transferencia se firma en el dispositivo del usuario con ML-DSA-44 (NIST FIPS 204), la firma se comprime en una prueba ZK-STARK —transparente, basada en hash y a su vez post-cuántica— y el contrato en cadena verifica la prueba, el nonce, el dominio y el plazo antes de liquidar. Cada operación puede llevar además una referencia ISO 20022 anclada como hash, lo que permite conciliación bancaria sin exponer datos sensibles.

1 000 M
SUPPLY MÁXIMO · SIN FUNCIÓN MINT

0,1 %
QUEMA EN CADA TRANSFERENCIA

~70 %
SUPPLY EN CONTRATOS PINKLOCK V2

0 · 0 · 0 · 0
HALLAZGOS CERTIK SKYNET · KYC SILVER

90 · 180 · 240
DÍAS DE STAKING · ×1 / ×1,3 / ×1,6

2 mainnets
TRANSFERENCIAS PQC EN BNB CHAIN Y ETHEREUM

Lo que este documento demuestra

- **De dónde venimos:** una tesis clara —el riesgo cuántico es un problema de hoy, no de 2035— y una empresa constituida en Costa Rica para atacarlo con productos, no con papers.
- **Lo que construimos:** el rail PQC + ZK, el token QRYP con quema, la QRYPTA Wallet con firma 2-de-2 ligada al dispositivo, el staking on-chain con referidos y la PQC Dapp pública.
- **Dónde estamos:** contrato verificado, auditoría pública, liquidez en PancakeSwap, listado en BNB DappBay, locks auditables y una fase de staking y gobernanza en ejecución.
- **Hacia dónde vamos:** auditoría de la wallet, servicios con QRYP dentro de la app, QRYPTA Exchange, integración con un neobanco en Qatar y la ruta —laboratorio, devnet, testnet, mainnet— de NEUROCHAIN.

> **La pregunta no es si el mercado necesitará seguridad post-cuántica. La pregunta es quién estará preparado cuando ese momento llegue.**

CAPÍTULO 02

De dónde venimos

QRYPTA® no nació como un token en busca de una narrativa. Nació como respuesta a una fecha límite conocida por toda la industria y como la primera apuesta de una fintech costarricense por competir en infraestructura financiera global.

La tesis fundacional

Los sistemas financieros actuales —tanto los bancarios como los descentralizados— fueron construidos para otra era criptográfica. La seguridad de una firma ECDSA depende de un problema matemático (el logaritmo discreto en curvas elípticas) que el algoritmo de Shor resuelve con eficiencia en un ordenador cuántico suficientemente grande. No es una hipótesis marginal: es la razón por la que el NIST, la NSA (CNSA 2.0), la Comisión Europea y los principales bancos centrales han publicado calendarios de migración. A ello se suma la amenaza *"cosechar ahora, descifrar después"*: el tráfico y las claves que se graban hoy podrán abrirse mañana.

Provident Quantum Tech partió de tres convicciones que siguen guiando cada decisión de producto:

- **La seguridad post-cuántica debe ser de producción, no de roadmap.** Un estándar que solo existe en una testnet no protege a nadie.
- **La seguridad no puede costar usabilidad.** Si proteger fondos exige que el usuario opere arquitecturas tortuosas, el usuario elegirá el riesgo. La complejidad debe resolverse en la wallet y en la prueba, no en la persona.
- **Las finanzas reales hablan ISO 20022.** Sin semántica bancaria —referencias, conciliación, evidencia de liquidación— ningún activo digital entra en una tesorería corporativa.

Cronología

Constitución y marca CUMPLIDO
Provident Quantum Tech S.R.L. se constituye en Costa Rica (cédula jurídica 3-102-965820). QRYPTA se inscribe en el Registro Nacional (Nº 419244, clases 9, 36 y 42, vigente hasta 2036).

Infraestructura base CUMPLIDO
Contratos desplegados, rail post-cuántico vivo y verificación ZK activa. Primeras transferencias ZK + ML-DSA-44 registradas en BNB Chain y en Ethereum (transacciones Génesis, Anexo A).

Capa wallet CUMPLIDO
QRYPTA Wallet beta: autocustodia, multichain (BNB, ETH, BTC, SOL, TRON), smart accounts ERC-4337 y copiloto IA LUMI.

Endurecimiento de seguridad CUMPLIDO
Auditoría CertiK Skynet con 0 hallazgos críticos, mayores, medios o menores. Equipo verificado KYC Silver.

Activación del token CUMPLIDO
QRYP vivo en PancakeSwap v2, quema del 0,1 % operativa, listado en BNB DappBay, GeckoTerminal y DexScreener. Cerca del 70 % del supply custodiado en PinkLock v2.

Staking y gobernanza EN EJECUCIÓN
Staking on-chain de 90 / 180 / 240 días vivo. Contrato de referidos, fondeo del pool de recompensas y primeros parámetros de gobernanza en despliegue.

Por qué Costa Rica, por qué ahora

Costa Rica combina estabilidad institucional, talento técnico bilingüe y un marco societario claro. Provident Quantum Tech es la primera startup del país en llevar un token con infraestructura post-cuántica a producción; la elección no fue solo de origen sino de diseño: el equipo integra criptografía, operaciones bancarias, asesoría legal y gestión de riesgo, con la meta explícita de operar en mercados regulados y de expandirse desde San José hacia Doha, Europa y Asia.

Por qué Ethereum y BNB Chain

Ethereum

Base institucional y ecosistema de investigación y seguridad. Es el entorno más observado del mercado y por tanto el mejor lugar para demostrar un estándar verificable de grado bancario. La transacción Génesis en Ethereum prueba que el rail PQC + ZK funciona con costos aceptables incluso en la red más exigente.

BNB Chain

Alcance, adopción y costos bajos: ideal para el uso frecuente, la experiencia fluida y el volumen. Es la red donde vive el contrato principal de QRYP, el pool de liquidez, el staking y los locks. Validar PQC + ZK aquí demuestra que el modelo resiste demanda real.

El reloj regulatorio

HITO	QUÉ SIGNIFICA PARA QRYPTA®
Ago 2024 · NIST FIPS 203 / 204 / 205	Se publican los primeros estándares post-cuánticos: ML-KEM, ML-DSA y SLH-DSA. QRYPTA® se construye exactamente sobre esos tres.
Nov 2024 · NIST IR 8547	Ruta de transición: los esquemas clásicos de 112 bits (ECDSA, RSA-2048) quedan desaconsejados en 2030 y prohibidos en 2035.
Hoy · Cosechar ahora, descifrar después	Todo lo que no esté protegido post-cuánticamente ahora podrá ser abierto después. Solo la autoridad PQC en producción ofrece protección efectiva.
Mainnet · QRYPTA®	El contrato de transferencia PQC con verificación ZK, el token con quema y los contratos de staking están vivos en BNB Chain; el rail también se validó en Ethereum.

Regla de oro desde el primer día. Cada avance arquitectónico se lleva a producción únicamente si puede ser auditado, verificado y respaldado en tiempo real. Ninguna cifra de este documento depende de una hoja de cálculo interna: se lee de la cadena.

CAPÍTULO 03

El problema que resolvemos

Tres fricciones frenan la entrada del volumen institucional a los activos digitales. QRYPTA® las trata como un único problema de diseño.

1 · Riesgo criptográfico terminal

Billones de dólares y redes enteras dependen de forma monolítica de ECDSA. Cuando un ordenador cuántico relevante exista, cada clave pública expuesta en cadena será un objetivo. Migrar una red viva después del hecho es órdenes de magnitud más caro que diseñarla bien desde el inicio.

2 · Seguridad frente a fricción

Hasta ahora, reforzar la seguridad significaba trasladar la carga al usuario: firmas ciegas de calldata opaco, semillas que valen todo, respaldos con un solo cifrado. La industria acepta como normal que una frase robada vacíe una wallet en segundos.

3 · Falta de semántica bancaria

Las tesorerías corporativas y los bancos se rigen por ISO 20022: identificadores end-to-end, referencias de conciliación y evidencia de liquidación. Los modelos cripto primitivos ignoran ese lenguaje y con ello se autoexcluyen de los flujos B2B.

La respuesta de QRYPTA®

El proyecto no elige entre seguridad, usabilidad y cumplimiento: los resuelve en capas distintas para que ninguna comprometa a las demás. La **identidad** es post-cuántica (ML-DSA-44) y se registra on-chain. La **transacción** se demuestra con una prueba ZK y viaja con nonce, dominio y deadline, de modo que no hay firma a ciegas ni replay. El **dispositivo** aporta la segunda de dos firmas, protegida por hardware seguro y biometría. La **recuperación** usa un pack cifrado en cascada con gasto restringido tras restaurar. La **red** incorpora cripto-agilidad para migrar primitivas de forma gobernada. Y el **asistente** LUMI prepara pero nunca firma: el humano decide.

ESTÁNDAR DE LA INDUSTRIA	QRYPTA®
Firmas ECDSA / secp256k1, rompibles con el algoritmo de Shor	**Firmas en retículas ML-DSA-44 (NIST FIPS 204), verificadas on-chain vía ZK-STARK**
SNARK con ceremonias de trusted setup	**STARK: transparentes, basados en hash y post-cuánticos; sin ceremonia ni residuo tóxico**
Migración cuántica «planeada» para 2030+	**Autoridad post-cuántica en producción hoy en dos mainnets EVM**
Una semilla robada vacía la wallet	**Firma 2-de-2 ligada al dispositivo: la semilla sola no puede mover fondos**

ESTÁNDAR DE LA INDUSTRIA	QRYPTA®
Firma a ciegas de calldata opaco	**Decodificador en lenguaje claro; eth_sign bloqueado; detección de approvals ilimitados, Permit2 y typosquatting**
Respaldos con un solo cifrado	**Cascada ChaCha20-Poly1305 + AES-256-GCM, PBKDF2-SHA512 (80 000 iteraciones), gasto restringido tras restaurar**
Criptografía cableada en el protocolo	**Cripto-agilidad: identificadores de suite y migración gobernada de primitivas (NeuroShield)**
Sin semántica bancaria	**Referencias, hashes y evidencia de liquidación ISO 20022 anclados on-chain**
Auditoría pendiente o parcial	**CertiK Skynet: 0 críticos · 0 mayores · 0 medios · 0 menores · equipo KYC Silver**

CAPÍTULO 04

Lo que construimos: la arquitectura

Una sola base criptográfica sostiene cuatro productos. El principio es el mismo en todos: autoridad post-cuántica verificada con pruebas Zero-Knowledge y semántica ISO 20022 para las finanzas reales.

El rail PQC + ZK

QRYPTA® evita el error habitual de intentar verificar firmas post-cuánticas dentro de Solidity, donde su tamaño y costo serían prohibitivos. En su lugar delega el trabajo pesado al lugar correcto: la firma ML-DSA-44 se genera y se resguarda en el dispositivo del cliente, un *prover* la comprime en una prueba ZK-STARK que afirma "existe una firma válida sobre exactamente esta transferencia" y el contrato EVM únicamente verifica esa prueba ligera antes de ejecutar. El resultado es seguridad post-cuántica con un costo de gas compatible con el uso cotidiano.

El hash del mensaje encadena al remitente, destinatario, monto, nonce, identificador de cadena, dirección del token y el hash de la referencia ISO 20022. Con ello el rail garantiza tres barreras innegociables: registro riguroso de la identidad PQC (raíz pública registrada on-chain), veto absoluto a los ataques de repetición mediante nonce por clave, dominio de cadena y plazo de validez, y trazabilidad empresarial sin exponer datos sensibles en un ledger público.

Por qué STARK y no SNARK

Los STARK dependen únicamente de funciones hash resistentes a colisiones. No requieren emparejamientos de curvas elípticas —vulnerables al mismo adversario cuántico que se quiere neutralizar— ni ceremonias de *trusted setup* cuyo residuo tóxico pueda filtrarse. Con ello la prueba que protege la firma post-cuántica es, a su vez, post-cuántica: no hay un eslabón clásico escondido en la cadena de confianza.

Cuatro productos, un mismo núcleo

PRODUCTO	QUÉ ES	BASE CRIPTOGRÁFICA
Token QRYPTA®	BEP-20 / ERC-20 en BNB Chain y Ethereum, quema del 0,1 % en cada transferencia, modo de transferencia PQC	ML-DSA-44 · ZK-STARK · nonce / dominio / deadline · refs ISO 20022

PRODUCTO	QUÉ ES	BASE CRIPTOGRÁFICA
QRYPTA Wallet	Autocustodia multichain (BNB, ETH, BTC, SOL, TRON) con smart account ERC-4337 y firma 2-de-2	ERC-4337 · Secure Enclave / StrongBox · Guardián split · cascada AEAD
Staking y referidos	Contratos Solidity 0.8.28 + OpenZeppelin 5 en BNB Chain, plazos de 90 / 180 / 240 días, referidos on-chain	Contabilidad compatible con quema · no custodial · owner limitado a fondear y ajustar tasa
NEUROCHAIN	Layer 1 cognitiva y post-cuántica en diseño (desarrollo 2027)	ML-DSA + ML-KEM + SLH-DSA desde Génesis · NeuroBFT · NeuroISO

Suite criptográfica

Sin cifrados propietarios ni seguridad por oscuridad. Cada primitiva es un estándar publicado y revisado por pares, elegida para el rol exacto que cumple y con una ruta de migración documentada.

ALGORITMO	ESTÁNDAR	ROL EN QRYPTA®	POR QUÉ ESTA
ML-DSA-44 Dilithium2 · firmas en retículas · Nivel 2 NIST · PK 1 312 B · firma 2 420 B	NIST FIPS 204 (2024)	Identidad de la wallet y cada transferencia PQC	Recomendación principal del NIST para firma post-cuántica. Claves y firmas lo bastante pequeñas para móviles y anclaje on-chain; segura frente a Shor.
ZK-STARK FRI · basado en hash · sin trusted setup	Ben-Sasson et al.	Verificación on-chain de firmas PQC	Solo supuestos de hash; la prueba afirma que existe una firma válida sobre la transferencia exacta sin exponer nada más.
ML-KEM-768 Kyber · Nivel 3 NIST · PK 1 184 B · CT 1 088 B	NIST FIPS 203 (2024)	Sesiones nodo a nodo de NEUROCHAIN	Protege el tráfico entre validadores del «cosechar ahora, descifrar después»; claves rotadas por época.
SLH-DSA SPHINCS+ · firmas hash sin estado	NIST FIPS 205 (2024)	Raíces críticas, génesis y claves de gobernanza	Si los supuestos de retículas se debilitaran, la firma basada en hash sigue en pie: dos fundamentos independientes, una autoridad.
ChaCha20-Poly1305 + AES-256-GCM AEAD en cascada · 256 bits	RFC 8439 · SP 800-38D	Pack de recuperación y bóveda local	Dos AEAD de familias de diseño distintas; claves derivadas con PBKDF2-SHA512 a 80 000 iteraciones.
Hardware seguro · 2-de-2 Fail-closed · semilla sola = 0 de 2 firmas	Secure Enclave / StrongBox · TOTP RFC 6238	Toda operación que toca fondos	La segunda clave nunca sale del hardware del teléfono; en BTC, SOL y TRON el Guardián cofirma con clave enrolada, TOTP y time-lock.

Hash e integridad: SHA-256 / Keccak-256 en cadena y SHA-512 en la derivación de claves. Las referencias ISO 20022 se hashean y anclan on-chain; el payload sensible permanece cifrado fuera del ledger. ECDSA clásico se conserva únicamente como alias de compatibilidad, nunca como autoridad final.

Defensa en profundidad

Identidad

Identidad post-cuántica ML-DSA-44 registrada on-chain.

Transacción

Prueba ZK + nonce / dominio / deadline; sin firma a ciegas.

Dispositivo

Segunda clave en hardware seguro, biometría y contraseña maestra.

Recuperación

Pack cifrado, PDF imprimible, gasto restringido tras restaurar.

Red

Cripto-agilidad NeuroShield: migración gobernada de suites.

Asistente

LUMI prepara, nunca firma: el humano decide.

ISO 20022 como capa de contexto

ISO 20022 es el estándar global de mensajería de pagos y reporting, adoptado por SWIFT, los sistemas de pagos instantáneos y la mayoría de bancos centrales. En QRYPTA® cada transferencia puede llevar una referencia de tipo ISO 20022 que adjunta contexto empresarial: identificador end-to-end, motivo de pago, memo o referencia interna. En cadena, esa referencia se emite como hash y evento: auditable y verificable, pero sin exponer datos personales o comerciales.

Para tesorerías y bancos

Conciliación directa (straight-through processing) contra sus sistemas core, sin abandonar sus ventanas operativas. Habilitador de esquemas AML / KYC dictados por las cámaras bancarias.

Para el ledger

Semántica, hash, referencias y evidencia de liquidación on-chain; el payload sensible permanece cifrado fuera del ledger. El mismo principio rige la capa NeuroISO de NEUROCHAIN.

Ficha técnica del stack

Firmas digitales	ML-DSA-44 (Dilithium2, NIST FIPS 204) · ECDSA clásico solo como alias de compatibilidad
Sistema de pruebas	ZK-STARK: transparente, basado en hash, post-cuántico; verificado en la EVM
Redes (hoy)	BNB Chain · Ethereum · Base · Core · Polygon · Arbitrum (EVM) · Bitcoin · Solana · Tron

Modelo de cuenta	Smart account ERC-4337, firma 2-de-2 ligada al dispositivo, abstracción de gas
Cifrado en reposo	Cascada ChaCha20-Poly1305 + AES-256-GCM · PBKDF2-SHA512, 80 000 iteraciones
Intercambio de claves (NEUROCHAIN)	Sesiones nodo a nodo con ML-KEM · ML-DSA + SLH-DSA para raíces críticas
Consenso (NEUROCHAIN)	Admisión NeuroPoS · finalidad determinista NeuroBFT · multi-cliente
Semántica financiera	Referencias, hashes y evidencia de liquidación ISO 20022 en cadena; payload sensible off-chain
Auditoría y verificación	CertiK Skynet: 0 críticos / 0 mayores / 0 medios / 0 menores · equipo KYC Silver · listado en BNB DappBay

Principio de comunicación. QRYPTA® publica solo lo que puede verificarse: contratos verificados, transacciones Génesis, auditoría pública y locks legibles en cadena. Los superlativos de rendimiento de NEUROCHAIN se reservan para cuando existan testnet pública, metodología y benchmarks independientes.

CAPÍTULO 05

Productos en producción

Cuatro piezas del ecosistema operan hoy con contratos vivos en BNB Chain. Esta sección describe qué hace cada una, cómo se usa y qué reglas la gobiernan.

Token QRYPTA® · QRYP

BEP-20 en BNB Smart Chain (chainId 56), 18 decimales, supply máximo de 1 000 000 000 sin función de emisión. Quema del 0,1 % (burnRateBps = 10) en cada transferencia, permanente y visible en el supply total on-chain. Modo de transferencia PQC con firma ML-DSA-44 y verificación ZK. Auditado por CertiK; listado en PancakeSwap v2, GeckoTerminal, DexScreener y BNB DappBay.

QRYP en 60 segundos: tres usos reales

01 · Pagar con firma post-cuántica

Cada transferencia se firma con ML-DSA-44, se comprime en una prueba ZK-STARK y se verifica on-chain. El 0,1 % se quema en cada movimiento: cuanto más se usa, más escaso es. Disponible en la PQC Dapp pública.

02 · Stakear y ganar por sostener la red

Plazos de 90, 180 y 240 días con multiplicadores ×1, ×1,3 y ×1,6, APR y rendimiento diario en vivo, reclamo cada 30 días y recompensas por referidos pagadas por contrato. No custodial.

03 · Desbloquear servicios en la wallet

En QRYPTA Wallet, QRYP paga comisiones con descuento, activa el staking de tarjetas (Platinum, Gold, Diamond) y será el activo de liquidación del exchange y del neobanco de Qatar.

QRYPTA Wallet

Wallet no custodial para BNB, ETH, BTC, SOL y TRON con smart accounts ERC-4337 y firma 2-de-2: la semilla por sí sola nunca basta; el segundo factor vive en el hardware seguro del teléfono y se libera solo tras biometría y contraseña maestra. Para cadenas no-EVM, un servidor Guardián con clave de dispositivo enrolada, TOTP y time-lock cofirma los montos altos. La app incluye un decodificador de transacciones en lenguaje claro, bloqueo de *eth_sign*, detección de approvals ilimitados, Permit2 y typosquatting, navegador Web3 endurecido, swap y puente cross-chain (0x, Jupiter, LI.FI), programa de tarjetas y LUMI, el copiloto de IA que prepara operaciones pero nunca firma.

Recuperación

Pack de recuperación `.qrypta` cifrado dos veces con dos AEAD independientes (ChaCha20-Poly1305 + AES-256-GCM), claves derivadas con PBKDF2-SHA512 a 80 000 iteraciones; PDF imprimible y gasto restringido tras restaurar.

Matriz de seguridad por acción

Cada operación define qué factores exige: ver saldo, firmar un mensaje, mover fondos o cambiar guardianes tienen requisitos distintos. Fail-closed: ante duda, la operación no se ejecuta.

Staking on-chain (QryptaYieldStaking)

90	180	240
días · multiplicador ×1,0	días · multiplicador ×1,3	días · multiplicador ×1,6

- **Contabilidad por diferencia de balance:** el contrato registra exactamente los QRYP recibidos tras la quema del 0,1 %, evitando desajustes entre lo enviado y lo acreditado.
- **Acumulación por segundo:** las recompensas se devengan según `rewardRate` y el peso de cada posición (monto × multiplicador).
- **Reclamo cada 30 días;** el capital se retira al vencer el plazo. El APR mostrado se calcula en vivo desde la cadena.
- **No custodial:** solo la wallet del usuario puede retirar su posición. El owner únicamente fondea el pool y ajusta la tasa; no puede mover posiciones ajenas.

Referidos on-chain (QryptaStakingReferral)

PARÁMETRO	VALOR
Mínimo del referidor	150 QRYP en staking
Mínimo del referido	100 QRYP en staking
Recompensa del referidor	5 % (500 bps)
Recompensa del referido	2 % (200 bps)
Liquidación	Pagada por contrato; aviso de recompensa pendiente en la página de staking

PQC Dapp: la transferencia post-cuántica, en público

Cualquier usuario puede firmar una transferencia de QRYP con ML-DSA-44 desde el navegador, generar la prueba ZK y liquidarla en BNB Chain. La Dapp es la demostración viva del rail y el mismo flujo que la wallet ejecuta de forma nativa. Las dos transacciones Génesis —una en BNB Chain y otra en Ethereum— son verificables en los exploradores públicos (Anexo A).

Cómo adquirir QRYP

1. Instalar una wallet EVM (QRYPTA Wallet, MetaMask, Trust) y añadir la red BNB Smart Chain.
2. Disponer de BNB para gas y de USDT o BNB para el intercambio.
3. Abrir PancakeSwap y pegar el contrato exacto del token; comprobar que el símbolo sea QRYP.
4. Ajustar el slippage a 1–2 % (la quema del 0,1 % se aplica en cada transferencia).
5. Añadir el token a la wallet desde el botón oficial de la página de staking.

> **Seguridad.** Provident Quantum Tech nunca solicita la frase semilla, nunca envía enlaces por mensaje directo y nunca promete rendimientos fijos. Los anuncios oficiales se publican únicamente en providentquantum.tech y en @QRYPTARail. Cualquier dirección distinta a las del Anexo A es falsa.

CAPÍTULO 06

Dónde estamos: estado verificable

Instantánea on-chain al 8 de septiembre de 2026. Cada cifra se lee de BNB Chain y se actualiza en vivo en providentquantum.tech/qrypta.

999 735 212
SUPPLY ACTUAL (QRYP)

264 788
QUEMADO PARA SIEMPRE

702 902 310
BLOQUEADO EN PINKLOCK V2 · 70,3 %

~296,8 M
SUPPLY CIRCULANTE

0 / 0 / 0 / 0
CERTIK · CRÍTICOS / MAYORES / MEDIOS / MENORES

PancakeSwap v2
POOL QRYP / WBNB · PRECIO PÚBLICO

Qué está cumplido

Las cinco fases fundacionales del roadmap están completas: infraestructura base, capa wallet, endurecimiento de seguridad y activación del token, además de la constitución de la empresa y el registro de la marca. El contrato de QRYP está verificado en BscScan; la auditoría CertiK Skynet es pública y el equipo está verificado (KYC Silver); el token cotiza en un pool público de PancakeSwap v2, rastreado por GeckoTerminal y DexScreener, y aparece en BNB DappBay.

Qué está en ejecución

La fase actual es **Staking y gobernanza**. El staking on-chain de 90 / 180 / 240 días está vivo; se están desplegando el contrato de referidos, el fondeo del pool de recompensas y los primeros parámetros de gobernanza. En paralelo, la QRYPTA Wallet opera en beta con autocustodia y multichain.

Custodia del supply: locks PinkLock v2

Cerca del 70 % del supply está custodiado en el contrato PinkLock v2, un locker de terceros ampliamente utilizado y auditado. Cada lock —etiqueta, cantidad y fecha de desbloqueo— se lee en vivo desde BNB Chain en la sección "Bloqueos verificables" del sitio y puede auditarse de forma independiente en BscScan o PinkSale. El equipo publica el estado de cada lock (bloqueado, reclamable o retirado) sin edición: la transparencia se ejerce también cuando un plazo vence.

Principios que ya se cumplen

Transparencia

Contrato verificado en BscScan · locks legibles en vivo · auditoría CertiK con 0 hallazgos.

Liquidez real

Pool QRYP / WBNB en PancakeSwap v2 · listado en GeckoTerminal y DexScreener · sin market makers ocultos.

Incentivos alineados

Staking con plazos · referidos pagados por contrato · solo 8 % del supply para fundadores y equipo.

Resistencia a la manipulación

1 000 000 000 fijo · sin mint · quema automática del 0,1 % · parámetros públicos on-chain.

Verificación por terceros

ENTIDAD	QUÉ VERIFICA	DÓNDE
CertiK Skynet	Auditoría del contrato del token y monitoreo continuo: 0 críticos, 0 mayores, 0 medios, 0 menores. KYC Silver del equipo.	skynet.certik.com/projects/qrypta
BscScan	Código fuente verificado, supply, quema, transferencias, locks y contratos de staking.	bscscan.com/token/...8153
BNB DappBay	Listado oficial del ecosistema BNB Chain con verificación de proyecto.	dappbay.bnbchain.org/detail/qrypta
PinkSale · PinkLock v2	Registros de cada lock de supply: cantidad, etiqueta y fecha de desbloqueo.	bscscan.com/token/...8153?a=0x4079...1BBE
GeckoTerminal · DexScreener	Precio, liquidez y volumen del pool QRYP / WBNB en tiempo real.	geckoterminal.com/bsc/pools/...
Registro Nacional de Costa Rica	Marca QRYPTA® Nº 419244, clases 9, 36 y 42, vigente hasta 2036.	rnpdigital.com

Portafolio de la empresa y su estado

PRODUCTO	DESCRIPCIÓN	ESTADO
Token QRYPTA®	BEP-20 con quema nativa, staking sin custodia, referidos y transferencias ZK + ML-DSA-44.	EN PRODUCCIÓN

PRODUCTO	DESCRIPCIÓN	ESTADO
QRYPTA Wallet	Wallet multicadena post-cuántica con LUMI, swap, puente, staking de tarjetas y tarjetas Platinum / Gold / Diamond.	BETA
Staking y referidos	Contratos QryptaYieldStaking y QryptaStakingReferral en BNB Chain.	EN PRODUCCIÓN
PQC Dapp	Transferencias post-cuánticas desde el navegador.	EN PRODUCCIÓN
Neobanco · Qatar	Integración bancaria: rampas fiat y liquidación ISO 20022 para QRYP.	INTEGRACIÓN
Entretenimiento digital	QRYP como riel de pago para tres plataformas, liquidado vía wallet con privacidad ZK.	INTEGRACIÓN
QRYPTA Exchange	Exchange post-cuántico sobre el núcleo de seguridad de la wallet.	POST-WALLET
NEUROCHAIN	Layer 1 propia, post-cuántica por defecto, para liquidación bancaria y aplicaciones nativas de IA.	DISEÑO · 2027

Nota sobre listados. Provident Quantum Tech no mantiene por el momento planes de listado en exchanges centralizados. La liquidez de QRYP se descubre en un pool público y se ampliará con el QRYPTA Exchange propio, según el roadmap del Capítulo 8.

CAPÍTULO 07

Economía del token QRYP

QRYP no es un token especulativo. Es el motor económico de una arquitectura post-cuántica diseñada para operar cuando la seguridad actual deje de ser suficiente. Su modelo rehúye la emisión irrestricta: oferta fija, quema automática y utilidad real.

Reserva de integración bancaria	200 000 000 · 20 %
Staking, nodos y seguridad de red	180 000 000 · 18 %
Socios estratégicos e institucionales	150 000 000 · 15 %
Liquidez DEX y CEX	120 000 000 · 12 %
Ecosistema Wallet	100 000 000 · 10 %
Ecosistema y grants	100 000 000 · 10 %
Fundadores y equipo	80 000 000 · 8 %
Marketing, asesores y KOLs	60 000 000 · 6 %
Asignación comunitaria	10 000 000 · 1 %

Parámetros del contrato

Nombre · símbolo	QRYPTA® · QRYP
Estándar · red	BEP-20 · BNB Smart Chain (chainId 56) · ERC-20 en Ethereum para el rail PQC
Decimales	18
Supply máximo	1 000 000 000 QRYP · sin función mint
Quema por transferencia	0,1 % (burnRateBps = 10) · permanente · reduce el supply total on-chain
Modo PQC	quantumTransfer: firma ML-DSA-44 + prueba ZK + nonce / dominio / deadline + referencia ISO 20022
Gobernanza de parámetros	Contratos controlados por multisig; parámetros públicos verificables en cadena

Mecanismo deflacionario

Cada transferencia de QRYP destruye el 0,1 % del monto transferido. La quema es una obligación del contrato, no una política discrecional: no puede desactivarse desde una interfaz ni depende de la tesorería. Como el staking, los pagos dentro de la wallet, el exchange y las rampas bancarias generan transferencias, la actividad del ecosistema reduce estructuralmente la oferta. El sitio oficial incluye un simulador de deflación que proyecta el supply según el volumen transferido.

Distribución del supply

ASIGNACIÓN	TOKENS	PESO	FINALIDAD
Reserva de integración bancaria	200 000 000	20 %	Liquidez y garantías para rampas fiat, neobanco de Qatar y liquidación ISO 20022
Staking, nodos y seguridad de red	180 000 000	18 %	Pool de recompensas del staking, futuros attesters y validadores de NEUROCHAIN
Socios estratégicos e institucionales	150 000 000	15 %	Alianzas, integraciones institucionales y socios de distribución
Liquidez DEX y CEX	120 000 000	12 %	Pool QRYP / WBNB y liquidez del QRYPTA Exchange
Ecosistema Wallet	100 000 000	10 %	Incentivos de producto, tarjetas y servicios dentro de la wallet
Ecosistema y grants	100 000 000	10 %	Desarrolladores, SDK, hackathons e investigación
Fundadores y equipo	80 000 000	8 %	Equipo fundador, con bloqueo institucional
Marketing, asesores y KOLs	60 000 000	6 %	Posicionamiento global, asesores y creadores
Asignación comunitaria	10 000 000	1 %	Airdrops y recompensas de comunidad anunciados por canales oficiales
Total	**1 000 000 000**	**100 %**	

Solo 8 % del supply corresponde a fundadores y equipo, una de las asignaciones más bajas del sector.

Cerca del 70 % del supply está custodiado en contratos PinkLock v2, verificable en vivo en el sitio oficial y en BscScan.

Utilidad del token

FUNCIÓN	DESCRIPCIÓN
Motor de comisiones	Pago de tarifas del ecosistema con descuento de hasta 20 % cuando se liquida en QRYP.
Mecanismo de quema	0,1 % de cada transferencia se destruye; parte de las comisiones del rail PQC también se queman.
Staking y seguridad	Participación en la red mediante staking con plazos; base del futuro modelo de attesters y validadores.

FUNCIÓN	DESCRIPCIÓN
Servicios en la wallet	Staking de tarjetas (Platinum, Gold, Diamond), rutas de swap y pagos asistidos por LUMI.
Activo de liquidación	Unidad de valor del QRYPTA Exchange, del neobanco de Qatar y de las plataformas de entretenimiento digital.
Gobernanza	Evolución progresiva del protocolo y ajuste de parámetros vía DAO, a partir de la fase en ejecución.

Principios de diseño

La estructura de QRYP prioriza cuatro propiedades: **transparencia** (todo lo que se afirma puede leerse en cadena), **liquidez real** (precio descubierto en un pool público, sin market makers ocultos), **incentivos alineados** (quien sostiene la red gana con ella) y **resistencia a la manipulación** (supply fijo, sin emisión, quema automática y reglas escritas en el contrato).

Objetivos de tracción

Los siguientes indicadores son objetivos de gestión, no métricas actuales, y se publican para que la comunidad pueda medir la ejecución del equipo contra sus propios compromisos.

Crecimiento de holders

Ampliar la base de tenedores de forma orgánica a través de la wallet, el staking y las integraciones de pago, con foco en usuarios activos y no en direcciones vacías.

Volumen diario

Aumentar el volumen transferido —y con él la quema— mediante los servicios dentro de la wallet, el exchange propio y las rampas bancarias.

Ciclo económico

El diseño cierra un ciclo continuo entre uso, demanda y reducción de oferta: cada interacción dentro del sistema —una transferencia PQC, un pago con descuento, una posición de staking, una liquidación bancaria— exige QRYP, genera una quema y refuerza los incentivos de quienes sostienen la red. La demanda es utilitaria y creciente; la oferta es fija y decreciente.

Compromisos económicos del emisor

- No existe ni existirá función de emisión adicional de QRYP.
- La quema del 0,1 % es una regla del contrato y no una política revisable.
- Los locks de supply y su estado se publican sin edición, en vivo y con enlaces a registros públicos.
- Los contratos del ecosistema se controlan con multisig y se someten a auditoría externa antes de manejar fondos de usuarios.

- Las fechas del roadmap se anuncian únicamente por canales oficiales, cuando cada hito está verificado.

CAPÍTULO 08

Hacia dónde vamos

El orden es el compromiso; las fechas se anuncian solo por canales oficiales cuando cada hito está verificado. De infraestructura viva a una Layer 1 post-cuántica.

Staking y gobernanza EN EJECUCIÓN
Contrato de referidos, fondeo del pool de recompensas y primeros parámetros de gobernanza.

Auditoría de la wallet
Auditoría externa completa de QRYPTA Wallet: núcleo PQC, smart account 2-de-2, Guardián y pack de recuperación.

Servicios con QRYP dentro de la wallet
Utilidades nativas del token en la app: descuentos en comisiones, staking de tarjetas, rutas de swap y pagos asistidos por LUMI.

Expansión de marketing
Campañas globales, KOLs, hackathons y relaciones públicas institucionales posicionando a QRYPTA® como el estándar post-cuántico.

QRYPTA Exchange
Lanzamiento del exchange con QRYP como activo de liquidación y custodia post-cuántica, construido sobre el núcleo de seguridad de la wallet.

Integración con el neobanco · Qatar
Rieles ISO 20022 que conectan la wallet y QRYP con el neobanco de Qatar para rampas fiat de entrada y salida.

Testnet de NEUROCHAIN
Testnet pública: faucet tNEURO, validadores, cuentas PQC y adaptador EVM.

Pruebas públicas
Pruebas adversariales, multi-cliente, benchmarks independientes y auditorías antes de mainnet.

Mainnet de NEUROCHAIN
Layer 1 permissionless: post-cuántica desde el Génesis, finalidad NeuroBFT, ISO 20022 nativo. Ruta de migración para QRYP y todo el stack.

Roadmap corporativo

PERIODO	ETAPA	ALCANCE	ESTADO
2025 – 2026	**Fundación**	Empresa constituida, marca QRYPTA®, token en BNB Chain, auditoría CertiK, DappBay, liquidez, staking activo.	COMPLETADO

PERIODO	ETAPA	ALCANCE	ESTADO
2026	**Wallet y rieles**	Lanzamiento público de QRYPTA Wallet, programa de tarjetas, neobanco en Qatar y socios de entretenimiento digital.	EN CURSO
2026 – 2027	**Exchange**	QRYPTA Exchange sobre el núcleo post-cuántico de la wallet e incorporación institucional.	SIGUIENTE
2027	**NEUROCHAIN**	Blockchain propia, post-cuántica por defecto. Migración de QRYP y del stack de productos.	PLANIFICADO

El ecosistema que se completa

QRYP es la unidad de valor. La wallet es la puerta de entrada. El exchange y NEUROCHAIN son la infraestructura. La banca y el entretenimiento digital son los rieles de adopción. Cada pieza nueva aumenta la demanda utilitaria del token sin alterar sus reglas de emisión.

QRYPTA Exchange

Exchange post-cuántico construido sobre el núcleo de seguridad de la wallet: custodia con firma 2-de-2, QRYP como activo de liquidación y descuentos en comisiones. Arranca cuando la wallet esté plenamente operativa y auditada.

Neobanco · Qatar

Integración en curso con un neobanco con sede en Qatar: rampas fiat de entrada y salida y liquidación ISO 20022 para QRYP. Es la primera puerta de QRYPTA® hacia la banca regulada del Golfo.

Programa de tarjetas

Tarjetas Platinum, Gold y Diamond activadas mediante staking de QRYP dentro de la wallet; un puente cotidiano entre el activo digital y el gasto real.

Entretenimiento digital

QRYP como riel de pago para tres plataformas de entretenimiento digital, liquidado a través de la wallet con privacidad ZK.

NEUROCHAIN: la Layer 1 cognitiva y post-cuántica

NEUROCHAIN no es una colección de funciones sino una única Layer 1 diseñada alrededor de seis capacidades simultáneas. Agregarlas después crea fricción, deuda técnica y dependencias que degradan las garantías originales; por eso se diseñan juntas desde el Génesis. El desarrollo está programado para 2027 y el diseño se documenta en el *NEUROCHAIN Strategic & Technical Architecture Dossier v0.1* (agosto 2026).

PILAR	QUÉ GARANTIZA
PQC y cripto-agilidad	ML-DSA, ML-KEM y SLH-DSA desde el Génesis; migración gobernada entre suites (NeuroShield).

PILAR	QUÉ GARANTIZA
IA nativa	Un NeuroAgent dentro de cada validador: análisis, atestaciones firmadas y defensa. Nunca árbitro del consenso.
200K SFTPS	Objetivo de ingeniería en transacciones seguras y finalizadas por segundo: validadas, ejecutadas, comprometidas y finalizadas. No TPS brutas.
Descentralización	Proof of Stake permissionless para admisión (NeuroPoS), NeuroBFT para finalidad determinista, multi-cliente por diseño.
ISO 20022 nativo	Capa financiera NeuroISO: semántica, hashes, referencias y evidencia de liquidación on-chain; payload sensible fuera del ledger.
NeuroImmune	Detectar, aprender, actualizar y revertir sin downtime. Rollback de software, nunca de bloques finalizados.

Decisiones fundacionales de NEUROCHAIN

PREGUNTA	DECISIÓN	CONDICIÓN DE SEGURIDAD
¿PoW o PoS?	NeuroPoS para admisión + NeuroBFT para finalidad	La selección económica no sustituye las reglas BFT
¿La IA manda sobre el consenso?	No. Los NeuroAgents analizan y atestiguan	La validez base sigue siendo determinista
¿Direcciones 0x nativas?	No. neuro1... es el namespace nativo	0x... queda como alias / capa de compatibilidad
¿PQC añadido después?	No. PQC desde Génesis	La cripto-agilidad permite migrar en el futuro
¿ISO 20022 completo on-chain?	No. Semántica + hash + referencias + liquidación	Payload sensible cifrado fuera del ledger
¿Actualización automática desde un nodo?	Nunca unilateral	Reproducción independiente + quórum + canary
¿Rollback de cadena?	No	Rollback de software, nunca de bloques finalizados
¿200K TPS como afirmación inicial?	No. Objetivo de ingeniería	Publicar solo SFTPS medido y reproducible
¿GPU potente = más votos?	No	La capacidad de IA no compra poder de consenso

Camino a mainnet y financiamiento por hitos

ETAPA	ALCANCE	RANGO DE PLANIFICACIÓN
LAB-01	4 validadores locales + IA + explorer + benchmark. Génesis, cuentas PQ, bloque #0.	USD 10K – 50K
DEVNET	20+ nodos en varias regiones, integraciones de wallet, SDK, adaptador EVM.	USD 250K – 750K
TESTNET PÚBLICA	50–500 validadores, faucet tNEURO, staking, auditorías, carga WAN.	USD 1M – 2M
PERF TESTNET	Pruebas adversariales, multi-cliente, benchmarks reproducibles.	—
MAINNET	Infraestructura de producción, verificación formal, integraciones institucionales. Permissionless.	USD 3M – 7M

El laboratorio demuestra el núcleo, la devnet demuestra distribución, la testnet demuestra resiliencia adversarial, y las auditorías y benchmarks abren el capital de mainnet. Los rangos son estimaciones de planificación, no cotizaciones.

> **Límite de divulgación.** Este capítulo resume un documento conceptual. Omite deliberadamente la lógica de selección de comités, los formatos definitivos de mensajes de consenso, umbrales internos, derivación de claves, políticas de slashing y configuraciones de producción. No es código fuente, auditoría, especificación final de consenso ni promesa de rendimiento.

CAPÍTULO 09

Gobernanza, cumplimiento y empresa

Construida en Costa Rica. Diseñada para mercados regulados. La gobernanza es compliance-first: contratos controlados por multisig, auditorías públicas y parámetros verificables en cadena.

Entidad legal	Provident Quantum Tech S.R.L. · sociedad de responsabilidad limitada · Costa Rica · cédula jurídica 3-102-965820
Marca	QRYPTA® · Registro Nacional de Costa Rica Nº 419244 · clases 9, 36 y 42 · vigente hasta 2036
Gobernanza técnica	Contratos controlados por multisig · auditoría CertiK · parámetros públicos on-chain
Estándares	NIST FIPS 203 / 204 / 205 · ISO 20022 · ERC-4337 · OpenZeppelin 5
Canales oficiales	providentquantum.tech · @QRYPTARail (X) · t.me/qrypta_oficial · github.com/qryptalabs
Correo	contact@providentquantum.tech · contact@qryptalabs.com

Modelo de gobernanza

La gobernanza avanza de forma progresiva. En la fase actual, los parámetros económicos (tasa de recompensas, fondeo del pool) se administran por multisig y se publican en cadena; los contratos que tocan fondos de usuarios son no custodiales y no permiten al operador mover posiciones ajenas. La siguiente etapa incorpora la participación de los tenedores en el ajuste de parámetros vía DAO y, con NEUROCHAIN, un modelo de actualizaciones gobernadas —reproducción independiente, quórum, despliegue por canarios— en el que ninguna actualización es unilateral.

Arquitectura abierta y auditable

Sin el aval continuo del ecosistema técnico internacional no existe blindaje post-cuántico confiable. Las capas fundamentales del rail y de la liquidez se someten a auditoría externa y a revisión pública; las primitivas criptográficas son estándares publicados y las direcciones oficiales se documentan en este Libro Blanco y en el sitio. La wallet será objeto de una auditoría externa completa antes de su lanzamiento general.

Equipo fundador

Osbel Perera Álvarez
Director Ejecutivo (CEO) y Fundador
Lidera el desarrollo de una infraestructura financiera de próxima generación que combina seguridad post-cuántica, IA y blockchain.

Ernestina Mena Vilchis
Cofundadora
Colidera la ejecución y garantiza la alineación entre tecnología, estrategia comercial y expansión de mercado.

Erick Elías Bulgin
Cofundador y Director de Tecnología (CTO)
Lidera la arquitectura técnica de QRYPTA®, garantizando escalabilidad, seguridad e innovación.

Roy Álvarez
Cofundador · Jefe de Cumplimiento y Riesgos
Garantiza la alineación regulatoria y la gestión de riesgos en todo el protocolo.

Héctor Mario Soto Chaves
Cofundador · Gestor de Tesorería
Gestiona los recursos financieros y la estrategia de asignación de tokens.

Aymara Alonso Olivera
Cofundadora · Directora Legal
Lidera la estrategia legal y el marco regulatorio, asegurando un crecimiento escalable y conforme a la norma.

Cumplimiento y prevención de fraude

- **Identidad del emisor verificada:** el equipo completó la verificación KYC Silver de CertiK; la entidad legal y la marca son públicas y consultables.
- **Comunicación oficial única:** anuncios, direcciones de contrato y enlaces de descarga se publican exclusivamente en providentquantum.tech y en los canales listados. Ningún miembro del equipo solicita frases semilla ni envía enlaces por mensaje directo.
- **Sin promesas de rendimiento:** el APR del staking se calcula en vivo desde la cadena y depende del fondeo del pool y de la participación; no se garantizan rendimientos fijos.
- **Semántica AML / KYC preparada:** las referencias ISO 20022 ancladas en cadena permiten a bancos y tesorerías aplicar sus propios controles de cumplimiento sin exponer datos en el ledger.
- **Propiedad intelectual:** QRYPTA® es marca registrada. Toda reproducción no autorizada de logotipos, materiales de marca o contenido será objeto de acciones legales.

Cómo participar

Inversores y tenedores

Adquirir QRYP en el pool oficial, hacer staking on-chain y seguir el estado verificable en el sitio.

Instituciones

Integraciones bancarias, rampas fiat, liquidación ISO 20022 y custodia post-cuántica.

Desarrolladores y validadores

Documentación técnica, ABIs y flujo PQC en providentquantum.tech/docs; programa de validadores de NEUROCHAIN.

> **No estamos construyendo un token. Estamos construyendo una capa donde el valor es más seguro, más verificable y más alineado con el mundo real.**

CAPÍTULO 10

Riesgos y aviso legal

Este documento tiene fines informativos. No constituye oferta pública de valores, invitación a invertir, asesoría financiera, legal o fiscal, ni promesa de rendimiento.

Riesgos de mercado

El precio de QRYP se descubre en un mercado público y puede experimentar alta volatilidad, baja liquidez en determinados momentos y pérdidas totales o parciales del capital. La quema del 0,1 % reduce la oferta pero no garantiza apreciación. El desbloqueo de tokens custodiados en lockers puede afectar la oferta circulante.

Riesgos tecnológicos

Aunque los contratos han sido auditados y las primitivas criptográficas son estándares del NIST, ningún sistema es inmune a vulnerabilidades no descubiertas, errores de implementación, fallos de las redes subyacentes (BNB Chain, Ethereum) o de terceros (lockers, exploradores, agregadores). Los estándares post-cuánticos son recientes y su criptoanálisis continúa; la cripto-agilidad del diseño mitiga, pero no elimina, este riesgo.

Riesgos operativos y de ejecución

El roadmap describe el orden de los hitos, no compromisos de fecha. La QRYPTA Wallet opera en beta y será auditada externamente; el QRYPTA Exchange, la integración bancaria en Qatar y NEUROCHAIN dependen de desarrollo, financiamiento por hitos, socios y autorizaciones que pueden retrasarse o no materializarse. Las cifras de rendimiento de NEUROCHAIN son objetivos de ingeniería.

Riesgos regulatorios

La regulación de activos digitales evoluciona en Costa Rica, Qatar y el resto de jurisdicciones relevantes. Cambios normativos podrían restringir la disponibilidad de productos, exigir licencias adicionales o afectar la operación de socios. Cada usuario es responsable de cumplir las leyes de su jurisdicción, incluidas las obligaciones fiscales.

Riesgos de custodia

QRYP y la QRYPTA Wallet son no custodiales. La pérdida de la semilla, del dispositivo enrolado o del pack de recuperación puede implicar la pérdida irreversible de los fondos. Provident Quantum Tech no puede recuperar claves privadas ni revertir transacciones.

Declaración. Toda persona que adquiera, use o haga staking de QRYP declara haber leído y comprendido este capítulo y asume los riesgos descritos. Provident Quantum Tech S.R.L., sus fundadores y colaboradores no serán responsables por pérdidas derivadas del uso de los productos, de decisiones de inversión o de la actuación de terceros. Las declaraciones a futuro contenidas en este documento reflejan expectativas razonables a la fecha de publicación y pueden cambiar sin previo aviso.

Este Libro Blanco se publica en español e inglés. En caso de discrepancia prevalece la versión más reciente publicada en providentquantum.tech/whitepaper. Última revisión: septiembre de 2026.

CAPÍTULO A

Anexo: direcciones, referencias y glosario

Cualquier dirección distinta a las aquí listadas es falsa. Verifique siempre en el sitio oficial antes de operar.

Direcciones oficiales · BNB Smart Chain (chainId 56)

Contrato del token QRYP	`0x5266fe1aD9B035d0ED6142f1A70e9D6F102c8153`
Contrato de staking (QryptaYieldStaking)	`0xCa52c2603e53A24da10926a90D3BE19EAA6aA40b`
Locker PinkLock v2	`0x407993575c91ce7643a4d4cCACc9A98c36eE1BBE`
Pool PancakeSwap v2 (QRYP / WBNB)	`0x37755A004A7F84b030BE36036afbB0dbC3C0Ba5F`
Transacción Génesis · BNB Chain	`0x16984fc90a7de3231fff33db63420031ce26557b807415cdba0086cdcc7178aa`
Transacción Génesis · Ethereum	`0xf40b3665f19c9d1df309d203e2026f280d617fc6d1488763040c045de141a259`

Verificación y mercado

BscScan	`bscscan.com/token/0x5266fe1aD9B035d0ED6142f1A70e9D6F102c8153`
CertiK Skynet	`skynet.certik.com/projects/qrypta`
BNB DappBay	`dappbay.bnbchain.org/detail/qrypta`
GeckoTerminal	`geckoterminal.com/bsc/pools/0x37755a004a7f84b030be36036afbb0dbc3c0ba5f`
PancakeSwap	`pancakeswap.finance/swap?outputCurrency=0x5266fe1aD9B035d0ED6142f1A70e9D6F102c8153&chain=bsc`
Sitio oficial	`providentquantum.tech · /qrypta · /staking · /wallet · /neurochain · /docs`

Referencias normativas

- NIST FIPS 203 (2024): Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).
- NIST FIPS 204 (2024): Module-Lattice-Based Digital Signature Standard (ML-DSA).
- NIST FIPS 205 (2024): Stateless Hash-Based Digital Signature Standard (SLH-DSA).
- NIST IR 8547 (2024): Transition to Post-Quantum Cryptography Standards.

- Ben-Sasson, Bentov, Horesh, Riabzev (2018): Scalable, transparent, and post-quantum secure computational integrity (STARK).
- ISO 20022: Financial services — Universal financial industry message scheme. · ERC-4337: Account Abstraction Using Alt Mempool. · RFC 8439 · NIST SP 800-38D · RFC 6238.

Glosario

TÉRMINO	DEFINICIÓN
PQC	Criptografía post-cuántica: algoritmos diseñados para resistir ataques de ordenadores cuánticos.
ML-DSA-44	Esquema de firma digital sobre retículas (Dilithium2) estandarizado en FIPS 204; nivel de seguridad 2 del NIST.
ZK-STARK	Prueba de conocimiento cero escalable y transparente, basada solo en funciones hash; no requiere trusted setup.
Nonce / dominio / deadline	Contador por clave, identificador de cadena y token, y plazo de validez que impiden repetir o desviar una transferencia.
ISO 20022	Estándar global de mensajería financiera; en QRYPTA® se ancla como referencia hasheada en cada transferencia.
ERC-4337	Abstracción de cuentas en la EVM: cuentas inteligentes con lógica de firma programable y abstracción de gas.
2-de-2	Esquema en el que toda operación requiere dos firmas: la derivada de la semilla y la ligada al hardware del dispositivo.
PinkLock v2	Contrato de terceros para bloquear tokens con fecha de desbloqueo pública y verificable.
SFTPS	Secure Finalized Transactions Per Second: transacciones validadas, ejecutadas, comprometidas y finalizadas por segundo.
NeuroBFT / NeuroPoS	Finalidad determinista y mecanismo de admisión de validadores de NEUROCHAIN.

QRYPTA®

PROVIDENT QUANTUM TECH

La era cuántica necesita nuevos rieles. Los estamos construyendo, un producto a la vez.

providentquantum.tech
contact@providentquantum.tech · contact@qryptalabs.com
@QRYPTARail · t.me/qrypta_oficial · github.com/qryptalabs
San José, Costa Rica · Cédula jurídica 3-102-965820 · QRYPTA® N° 419244