COGNITUM™ — The Post-Quantum Layer-1

Quantum-safe by design. Not by patch.

*Public overview. This page is informational only — it is **not** an offer to sell or a solicitation to buy any security or token, and contains no offering terms. Any future participation is limited to qualified/eligible investors and is subject to securities-counsel review and applicable law in each jurisdiction.*

The thesis

Every major blockchain — Bitcoin, Ethereum, Solana — secures accounts with ECDSA, the elliptic-curve cryptography that Shor's algorithm on a sufficiently capable quantum computer breaks, recovering private keys from public keys already exposed on-chain. "Harvest-now, decrypt-later" makes it a present-tense problem: data and keys recorded today can be broken the day quantum matures. NIST has already standardized the replacement (FIPS 203/204/205) and is driving the migration.

COGNITUM is post-quantum from genesis — account security on ML-DSA65 (NIST FIPS 204), with SLH-DSA (FIPS 205) and ML-KEM-768 (FIPS 203). No ECDSA anywhere in account security. Not a retrofit, not a roadmap promise.

Why native beats retrofit

A chain with a live, trillion-dollar classical base can't migrate cleanly: every address that has spent has already exposed its public key (a permanent "harvested-key" tail no upgrade fixes retroactively); the transition requires multi-year coordination across thousands of wallets, exchanges, and custodians; and post-quantum signatures are 10–40× larger, breaking assumptions baked into block size, fees, and state. A chain that was **never classical** carries none of that. For long-lived, high-value assets — bonds, real estate, archival records — only PQ-from-genesis offers a signature that's still valid in 20–30 years.

Proof, not promises — verify it yourself

- **Live ledger integrity:** `curl https://api.cognitum.global/audit/run`

- **Post-quantum TLS, live:** `openssl s_client -groups X25519MLKEM768 -connect cognitum.global:443 -tls1_3`
- **No classical crypto in account security** — every signature is ML-DSA-65 (NIST FIPS 204).
- A full stack on testnet — DeFi, governance, protocol-level compliance, create-your-own-token, and 97-language access.

Honestly staged

COGNITUM is a **live single-operator testnet** today with self-auditable on-chain integrity and a full feature suite. It is **not decentralized yet** — independent validators, an external third-party audit, and mainnet are the published next phases. We tell you precisely what is and isn't done — because that is how we intend to steward trust.

> **Conservative by design:** "quantum-resistant," not "quantum-proof." A quantum computer capable of breaking ECDSA doesn't exist yet, and estimates range widely — from a few years in aggressive forecasts to ~10–15+ years in mainstream ones, with progress accelerating. You don't need to know the date: a shorter timeline makes native post-quantum security urgent, while a longer one still means assets signed today must outlive the threat. COGNITUM is built to win in either case. All on-chain metrics are independently verifiable.

For qualified investors

A detailed, confidential investor briefing — architecture, roadmap, economics, team, and round information — is available privately to qualified/eligible investors, subject to securities-counsel review.

Request the confidential briefing: support@cognitum.global
