NEUROVATIC, Inc. Completes 5-Layer Smart Contract Audit: Zero Critical Findings, External Review Scheduled

NEUROVATIC, Inc. announces the successful completion of a comprehensive five-stage internal security audit of its ValidatorRegistry smart contract, with an independent external audit by a top-tier global firm scheduled for Q2-Q3 2026.

Dover, Delaware Apr 13, 2026 (Issuewire.com) - **NEUROVATIC, Inc.**, the developer of NV-CHAIN and the world's first sovereign AI infrastructure layer, today announced the successful completion of a comprehensive five-stage internal security audit of its ValidatorRegistry.sol smart contract — the

foundational on-chain contract governing validator identity, staking, and governance rights on the NV-CHAIN network. The audit employed five independent validation methodologies across static analysis, property-based fuzzing, dual symbolic execution, and adversarial runtime simulation, returning zero critical or high-severity vulnerabilities.

The announcement signals a significant milestone in NEUROVATIC's ongoing commitment to institutional-grade security standards ahead of the company's planned external audit, to be conducted by a top-three globally recognized smart contract security firm, currently scheduled for Q2 2026.

Five Layers, Zero Critical Issues

The NEUROVATIC security team designed the Black Diamond audit pipeline as a mandatory, multi-layer validation framework applied automatically to every smart contract commit via continuous integration. The five-stage protocol is as follows:

Layer 1 — Static Analysis (Slither). ValidatorRegistry.sol was subjected to Slither, the industry-standard Solidity static analysis framework. The scan identified zero high-severity and zero medium-severity issues. Four low-severity informational findings were identified, all related to low-level native token transfer calls following the established Checks-Effects-Interactions (CEI) pattern with state variables zeroed prior to any external call. All four findings were reviewed, accepted, and formally documented.

Layer 2 — Property-Based Fuzzing (Echidna). Echidna, a property-based smart contract fuzzer, executed more than 150,000 randomized transaction sequences against formally defined invariants — including validator registration integrity, staking balance consistency, and access control boundaries. Zero invariant violations were recorded across the full fuzzing suite.

Layer 3 — Symbolic Execution (Mythril). Mythril performed exhaustive symbolic execution across all reachable execution paths in the EVM, using SMT solver-based constraint evaluation to identify integer overflows, reentrancy conditions, unauthorized asset transfer paths, selfdestruct exposure, and timestamp-dependency vulnerabilities. No exploitable issues were identified.

Layer 4 — Independent Symbolic Execution (Manticore). As a second independent symbolic execution engine, Manticore — developed by Trail of Bits — ran in parallel to eliminate tool-specific blind spots. Seven adversarial scenarios were explicitly targeted: reentrancy, integer overflow, access control bypass, front-running and MEV extraction, flash loan attack vectors, delegatecall injection, and self-destruct privilege escalation. All seven scenarios were fully mitigated. No exploitable paths were found.

Layer 5 — Adversarial Runtime Simulation (PyEVM). The contract was deployed and exercised within a fully instrumented Python EVM environment, simulating realistic adversarial conditions including multi-transaction attack sequences and coordinated front-running attempts. All invariants held under adversarial pressure. The contract passed all runtime simulation tests without exception.

Infrastructure: 9 Layers of Defense-in-Depth

The smart contract audit is one component of NEUROVATIC's broader security architecture, which applies nine layers of defense-in-depth across its entire N=12 BFT production cluster — twelve enterprise-grade dedicated nodes distributed globally across four continents (Europe, Asia-Pacific, US-West, US-East):

Application layer authentication uses HMAC-SHA256 with rotating shared secrets and ±60-second timestamp validation to prevent replay attacks. **Network layer** isolation enforces strict IP allowlisting on all BFT consensus endpoints. **Cloud and OS-level firewalls** apply a default-deny policy before any traffic reaches the application layer. **Intrusion prevention** systems (fail2ban) and **crowd-sourced threat intelligence** (CrowdSec) provide automated and proactive IP blocking. **SSH hardening** enforces Ed25519 key-only authentication — no password access is permitted to any production node. **TLS 1.3** with HSTS secures all public-facing endpoints via automated certificate management. **Cloudflare WAF and DDoS protection** absorbs volumetric and application-layer attacks at the global edge. **Continuous observability** via Prometheus, Grafana, and Uptime Kuma provides sub-60-second anomaly detection and alerting across the full cluster.

AEGIS: Quantum Security Sentinel

NEUROVATIC has deployed AEGIS — a dedicated post-quantum security monitoring system — across all production infrastructure nodes. AEGIS implements post-quantum cryptographic primitives based on NIST FIPS 203/204 standards (ML-KEM-768 and ML-DSA-65), providing quantum-resistant key encapsulation and digital signature verification across inter-node communication channels. AI inference nodes on the production cluster operate within bubblewrap (bwrap) sandboxes with full network isolation — structurally preventing any AI process from initiating unauthorized network activity, regardless of model behavior.

NPoI: Neural Proof of Intelligence

NV-CHAIN operates on Neural Proof of Intelligence (NPoI) — a proprietary consensus mechanism that replaces energy-intensive computational work with verifiable AI inference. Under NPoI, block finality requires consensus from 9 of the 12 cluster nodes, providing Byzantine fault tolerance of f=3 — meaning the network continues to operate correctly under the simultaneous compromise or failure of any three nodes. Block time is 10 seconds. The NPoI Patrol Agent audits validator authenticity continuously, in real time.

Neural-ID: Sovereign Digital Identity on NV-CHAIN

ValidatorRegistry.sol is the foundational layer for Neural-ID — NEUROVATIC's blockchain-native digital identity system. Each Neural-ID is an immutable, sovereign record anchored on NV-CHAIN, cryptographically bound to the holder's key pair without dependence on any central authority. The architecture is zero-knowledge proof compatible, enabling verifiable identity assertions without disclosure of underlying data. Every identity event — issuance, delegation, or revocation — is permanently recorded on NV-CHAIN with NPoI-validated finality.

Chain Architecture and Ecosystem Status

NV-CHAIN (Chain ID: 73790) is a fully independent, EVM-compatible sovereign blockchain, live on Chainlist.org and the DefiLlama chain registry. The network serves public traffic across five regional RPC endpoints. Block finality is deterministic — once 9 of 12 nodes converge, the block is mathematically irreversible, with no reorganization risk. Protocol-level MEV resistance is enforced at the consensus layer, not patched at the application level.

Intellectual Property

The core innovations underlying NV-CHAIN — including the NPoI consensus mechanism, the AEGIS

quantum security layer, Neural-ID, and the five-layer smart contract validation pipeline — are protected under 48 patent claims filed with the United States Patent and Trademark Office (USPTO) under provisional application NV-PAT-2026-001. NEUROVATIC™ is a registered trademark filed with OSIM Romania, with an international registration pathway via the Madrid System.

Executive Statement

"Security in AI-native blockchain infrastructure is not a feature — it is a prerequisite. The Black Diamond pipeline was built to ensure that every contract we deploy has been subjected to independent, adversarial validation before any user or partner depends on it," said Iulian Bondari, Founder and Chief AI Architect of NEUROVATIC, Inc. "Completing this audit with zero critical or high findings, across five independent methodologies and over 150,000 fuzz iterations, reflects the engineering discipline we apply to every layer of the stack. The upcoming external audit by a globally recognized firm will provide independent public verification of these results."

External Audit — Q2-Q3 2026

NEUROVATIC has initiated formal engagement with one of the top three globally recognized independent smart contract security firms for an external audit of the ValidatorRegistry.sol contract and the NV-CHAIN security architecture. The audit is scheduled for Q2 2026. Full results will be published upon completion. Qualified institutional partners may request access to existing internal audit documentation under a non-disclosure agreement.

About NEUROVATIC, Inc.

NEUROVATIC, Inc. is a Delaware C Corporation developing the world's first sovereign AI infrastructure layer — a convergence of advanced neural AI and blockchain technology. The company's core products include UNDECA-CORE (a 343.5M-parameter modular AI system), NV-CHAIN (Chain ID 73790, EVM-compatible sovereign blockchain with NPoI consensus), the AI Society governance platform, and Neural-ID. NEUROVATIC's infrastructure is deployed across twelve dedicated production nodes spanning four continents, serving institutional and developer users globally.

Website: https://neurovatic.ai
Explorer: https://explorer.neurovatic.ai
Developer Network: https://rpc.neurovatic.ai

Media Contact

Neurovatic, Inc.

*********@neurovatic.ai

1111B S Governors Ave # 99932

https://www.neurovatic.ai

Source : Neurovatic, Inc.

See on IssueWire