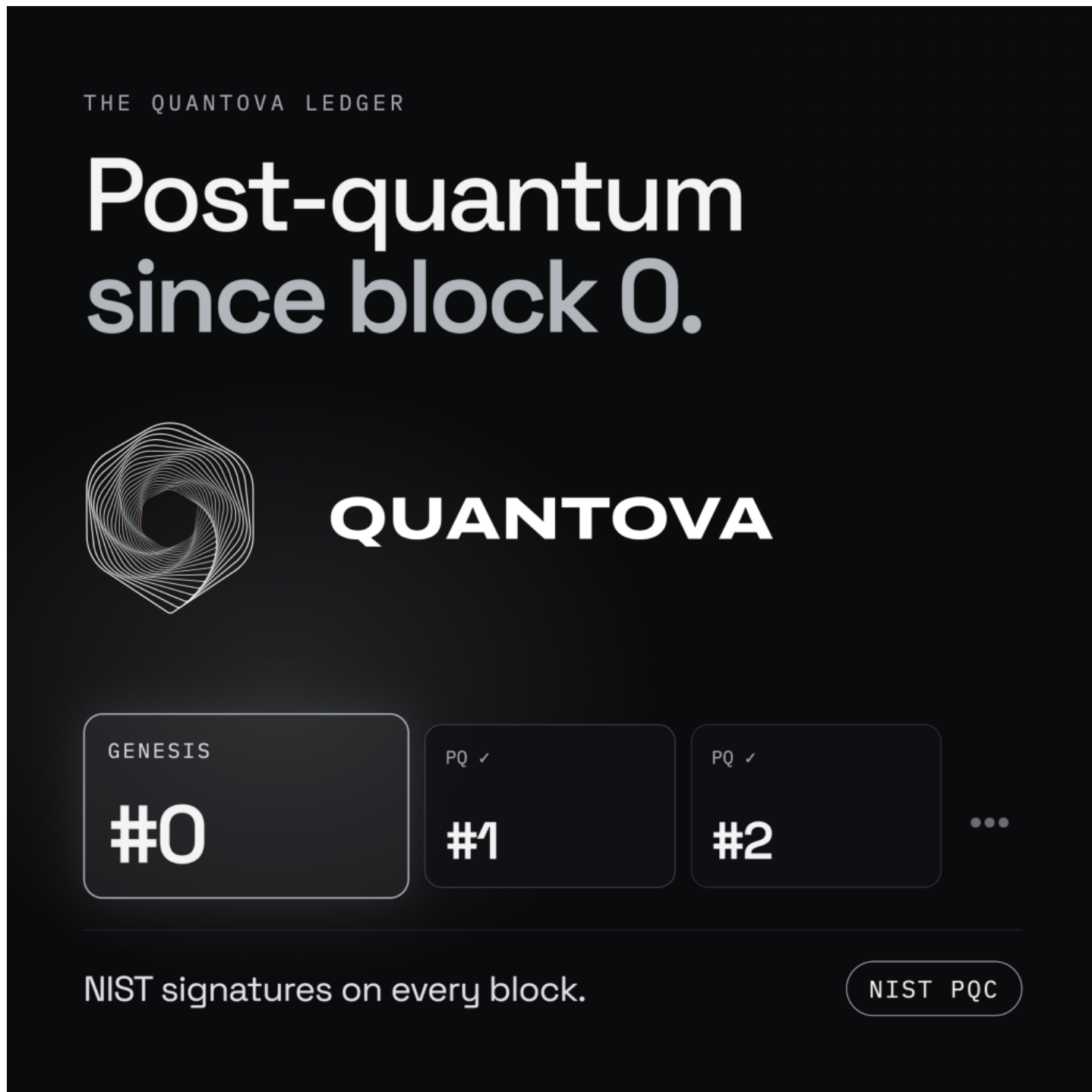


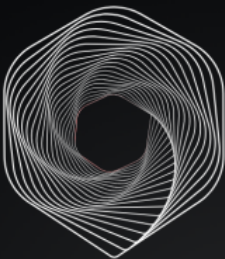
Quantova ledger has used NIST post quantum signatures since its first block

Every transaction and every finalized block on the Quantova network is signed with ML-DSA-65 under FIPS 204.



THE QUANTOVA LEDGER

Post-quantum since block 0.



QUANTOVA

GENESIS
#0

PQ ✓
#1

PQ ✓
#2

...

NIST signatures on every block.

NIST PQC

Wilmington, Delaware Oct 26, 2026 ([Issuewire.com](https://www.issuewire.com)) - [Quantova](https://www.quantova.com) operates a ledger built on NIST post quantum standards from its first block. Transactions are signed with ML-DSA-65 under FIPS 204, and the validator committee signs each block with the same algorithm to finalize it. NIST published FIPS 203, FIPS 204 and FIPS 205 on 13 August 2024.

Why the signatures matter

The NIST draft IR 8547 states that RSA, ECDSA and EdDSA are vulnerable to Shor's algorithm on a cryptographically relevant quantum computer. It proposes that quantum vulnerable algorithms be deprecated after 2030 and disallowed after 2035. For code signing, it advises that devices expected to verify signatures after such computers exist should require quantum resistant signatures. Long lived records face the same constraint, because a signature must stay verifiable for the retention period.

What Quantova built and runs

Quantova wrote its own [cryptography library](#), Q-Crypto, against the FIPS documents and tested it against the NIST known answer tests. It provides ML-DSA-65, ML-KEM-768 under FIPS 203 for key exchange, SLH-DSA under FIPS 205 and SHA3-256 under FIPS 202. The ledger uses SHA3-256 for its state trie, transaction roots and addresses. Grover's search algorithm gives a quantum computer a quadratic speedup against hash functions, which leaves a 256 bit hash such as SHA3-256 with about 128 bits of preimage security. Quantova also built its own contract language, Quanta, and its compiler, and the Quantova Virtual Machine, which verifies post quantum signatures natively.

As of 16 October 2026, the qvmScan.io explorer shows 4,601,535 finalized blocks, 26.27 million transactions processed and 116,584 addresses, with an average block time of about 0.2 seconds. The figures include Quantova's own load testing. Quantova has made public contributions to Ethereum, including ERC-8443 Quantum Bridge Shield and an EIP-8321 test fix, and to NEAR, Sui, TRON, BNB Chain, Cardano and the XRP Ledger, linked below.

Security review and disclosures

[Quantova](#) has signed a bug bounty programme with HackenProof, under which independent security researchers examine its code. The programme is not yet public. Quantova's implementations support FIPS 202, FIPS 203, FIPS 204 and FIPS 205. They have not been validated under FIPS 140-3 or the NIST Cryptographic Module Validation Program.

About Quantova

Quantova Inc builds a post quantum ledger on the NIST standards FIPS 202, FIPS 203, FIPS 204 and FIPS 205, and publishes the Qstamp SDK family for post quantum evidence. More information is available at [quantova.org](#) and [qstamp.org](#).

Media Contact

Quantova

*****@quantova.org

1000 N. West St., Ste. 1501

<http://quantova.org>

Source : Quantova Inc

[See on IssueWire](#)