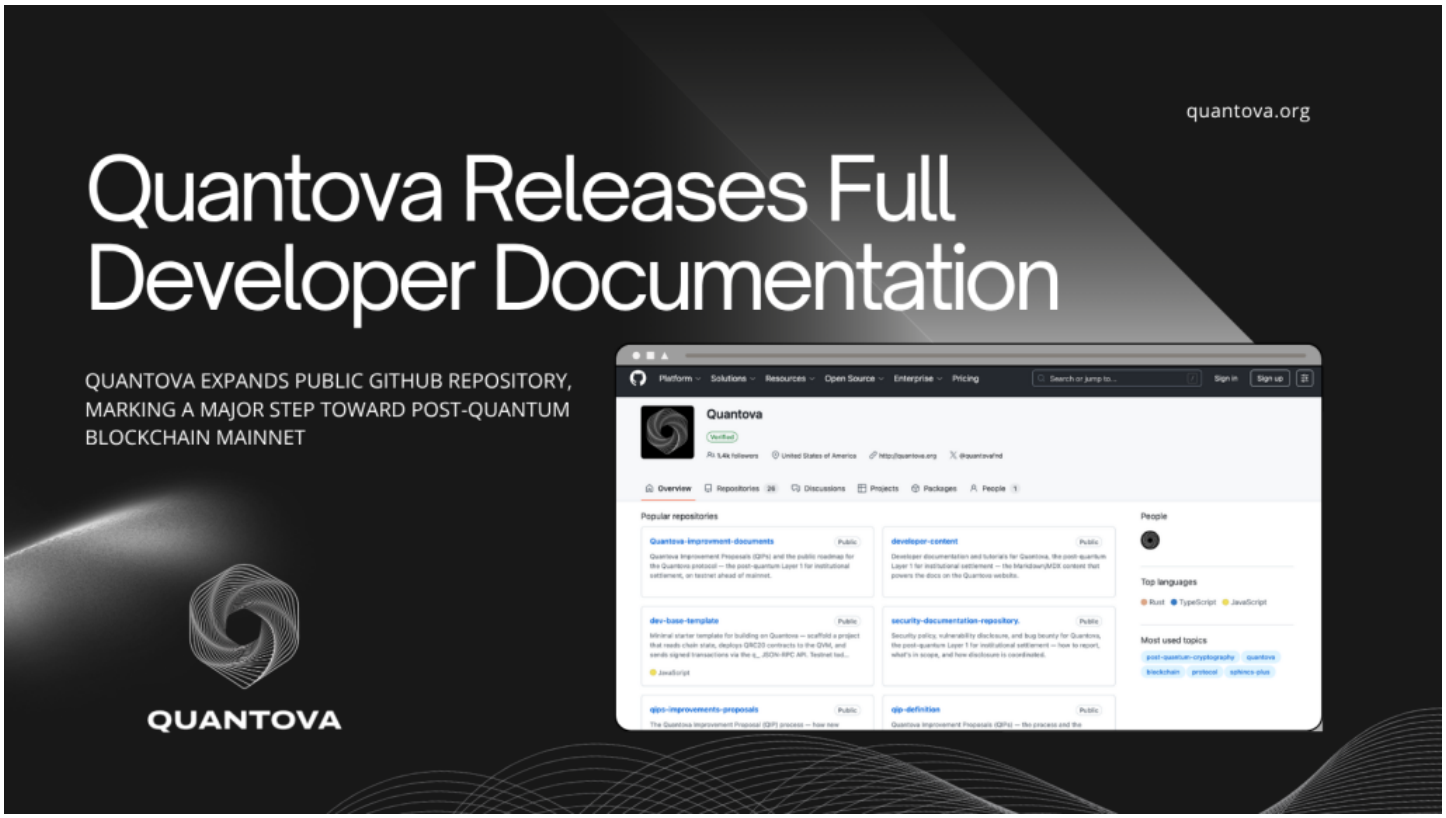
Quantova Releases Full Developer Documentation, Marking a Major Step Toward Post-Quantum Blockchain Mainnet

The post-quantum Layer-1 blockchain publishes its complete technical reference, publishes its consensus specifications, and formalises its governance framework on GitHub, accelerating developer access to the world's first Web4 execution layer.



Wilmington, Delaware Jun 10, 2026 (Issuewire.com) - Quantova, the post-quantum Layer-1 blockchain infrastructure company, today announced the public release of its comprehensive Developer Documentation v1.0 and a significant expansion of its public GitHub repository. The milestone marks a pivotal advancement in the project's march toward mainnet, giving developers, institutions, and researchers worldwide direct access to the technical foundations of the world's first quantum-resistant smart contract platform built from first principles.

The documentation release, covering the full protocol stack from post-quantum cryptographic primitives and account model through to the Quantova Virtual Machine (QVM), JSON-RPC reference, consensus mechanics, and node operation represents the most complete public technical disclosure in the project's history. It is published alongside a structured expansion of the Quantova repository, which now includes consensus specifications, a formalised Quantova Improvement Proposal (QIP) governance framework across dedicated repositories, the Quantova SDK, cross-chain bridge integration, and publicly available developer tooling.

"Releasing the full technical reference is not a documentation milestone — it is an infrastructure milestone. Every developer, institution, and researcher who reads this can now build directly on top of quantum-resistant cryptography without assembling it themselves. We are giving the world the tools to

build for what comes after classical blockchains."

— Founder, Quantova

The Post-Quantum Blockchain Problem

The global blockchain industry is built on elliptic-curve cryptography, ECDSA and related schemes that underpin Bitcoin, Ethereum, Solana, and virtually every major Layer-1 network in operation today. Shor's algorithm, executable on a sufficiently powerful fault-tolerant quantum computer, can recover an elliptic-curve private key from its public key in polynomial time. Because public keys are disclosed on-chain the moment an account first transacts, every spent wallet on every classical blockchain is, in principle, already a target.

The threat is not theoretical in the distant future. A strategy known as "harvest now, decrypt later" allows adversaries to record public keys and ciphertexts from public ledgers today and decrypt them once quantum hardware matures. Standards bodies have responded: the United States National Institute of Standards and Technology (NIST) finalised its first post-quantum cryptographic standards in 2024, standardising the lattice-based and hash-based signature schemes that Quantova has implemented at the protocol level since its inception.

Quantova was designed to eliminate this exposure entirely. Rather than retrofitting post-quantum security onto a classical architecture, Quantova engineers its cryptographic assumptions from first principles: every account, transaction, smart contract, and cross-chain bridge operation is secured by NIST-standardised post-quantum signature schemes, with SHA3-256 state hashing and a consensus mechanism that avoids quantum-vulnerable randomness.

What Quantova Published

The Developer Documentation v1.0 is a 46-page canonical technical reference covering the entire Quantova protocol. For developers, it provides a full SDK cookbook in JavaScript and Python, a JSON-RPC method reference for the **q_** namespace, the QVM execution model, Q primitive precompiles, Solidity contract examples, and node operation guides. For institutions and researchers, it documents the account and key derivation model, the Nominated Proof-of-Stake consensus architecture, the economic and fee model, tokenomics, governance referendum mechanics, and cross-chain bridge security properties.

On GitHub, the expansion covers six distinct areas of the Quantova publicly available GitHub presence: the formalised QIP governance framework published across dedicated repositories covering proposal definition, categories, contribution process, editor guidelines, and QVM integration enables the community to formally propose and ratify protocol changes. Consensus specifications are now publicly available. The Quantova SDK, built on the Substrate development framework, provides JavaScript and TypeScript tooling for post-quantum key management, chain queries, and QVM contract interaction. Developer tooling and a base template repository give builders a starting point for application development on the QVM.

"The QIP framework going live on GitHub signals that Quantova's governance is no longer a design document — it is an operational system. Protocol evolution now follows an transparent, auditable path from community proposal to on-chain referendum. No shortcuts. No admin keys."

— Quantova Core Engineering Team

Technical Architecture: Post-Quantum by Design

Quantova's cryptographic architecture rests on three NIST-standardised post-quantum signature schemes. CRYSTALS-Dilithium (ML-DSA) provides a balanced lattice-based scheme suitable for general-purpose accounts. Falcon (FN-DSA) delivers the smallest signature sizes of any NIST-standardised scheme and is used for validator authority keys. SPHINCS+ (SLH-DSA) offers the most conservative security assumptions through a stateless hash-based construction, optimal for high-assurance accounts. All three schemes derive into a single unified address space, with every account address beginning with the canonical prefix Q.

The Quantova Virtual Machine (QVM) executes Solidity-compiled smart contracts in a post-quantum execution environment. Native precompiles expose SHA3-256 hashing, post-quantum signature verification for all three NIST schemes, Q Threshold Encryption (QTE) for front-running-resistant transaction submission, and the Quantova Naming Service (QNS) directly to on-chain contracts. Validator authority keys use Falcon signatures. Slot leadership is deterministic round-robin rather than VRF-based, removing the elliptic-curve randomness dependency that classical Nominated Proof-of-Stake implementations carry. All state is committed to a SHA3-256 Merkle root.

Q Threshold Encryption (QTE) is an encrypted execution lane that prevents transaction front-running at the protocol level. A user encrypts their entire signed transaction with the network's current public encryption key before broadcasting it. The plaintext does not exist on-chain until after block finality — execution order is committed before any party can read the transaction contents. Decrypting a block early requires compromising a supermajority of validators, making sandwich attacks and MEV extraction structurally impossible rather than merely disincentivised.

Ecosystem and Use Cases

Quantova's execution environment supports the full spectrum of decentralised applications. Developers can deploy non-custodial financial systems where asset control and settlement logic are enforced by the QVM; issue protocol-level digital assets with deterministic supply rules; build decentralised identity frameworks that enable verification without centralised data custody; operate on-chain naming infrastructure through QNS; and construct cross-chain applications.

Governance: No Superuser, No Admin Key

A defining architectural property of Quantova is the complete absence of privileged administrative access. There is no sudo pallet, no superuser key, and no unilateral execution path available to any party including the founding team. Every protocol parameter change, runtime upgrade, and treasury action requires a bonded, time-locked, on-chain referendum with defined supermajority and quorum thresholds scaled to the impact of the proposed change.

The QIP framework, now live on GitHub, formalises how protocol improvement proposals move from community discussion to on-chain execution. Proposals covering consensus-critical parameters — including minting new QTOV or upgrading the runtime — require a minimum proposer stake of five to ten million QTOV locked for the governance cycle, an eighty percent supermajority, and quorum representing thirty-five to forty percent of circulating supply. This design makes governance capture expensive by construction.

Path to Mainnet

The documentation release and GitHub expansion are coordinated steps in Quantova's staged approach to mainnet deployment. The project has advanced its publicly accessible technical infrastructure across consensus specifications, SDK tooling, cross-chain bridge integration, and governance frameworks, each component independently reviewable and auditable by developers, security researchers, and institutions ahead of the mainnet launch.

"The internet is being re-architected. Centralised control is giving way to open, verifiable infrastructure. Quantova is where that transition meets quantum-resistant cryptography — the combination that makes Web4 possible."

— Quantova Team.

About Quantova

Quantova is an independent, post-quantum Layer-1 blockchain network and execution platform designed to provide deterministic and quantum-secure execution for governments, institutions, enterprises, and developers. The Quantova Virtual Machine (QVM) executes Solidity smart contracts in a natively post-quantum environment, enforcing NIST-standardised cryptographic standards — CRYSTALS-Dilithium, Falcon, and SPHINCS+ at the protocol level across all accounts, transactions, contracts, and bridges.

Website: quantova.org

Developer Docs: quantova.org/docs

GitHub: github.com/Quantova

Twitter / **X:** x.com/quantovafnd

Discord: discord.gg/aeKB42tx2

Media Contact

Quantova

*********@quantova.org

1000 N. West St., Ste. 1501

http://quantova.org

Source : Quantova Inc

See on IssueWire