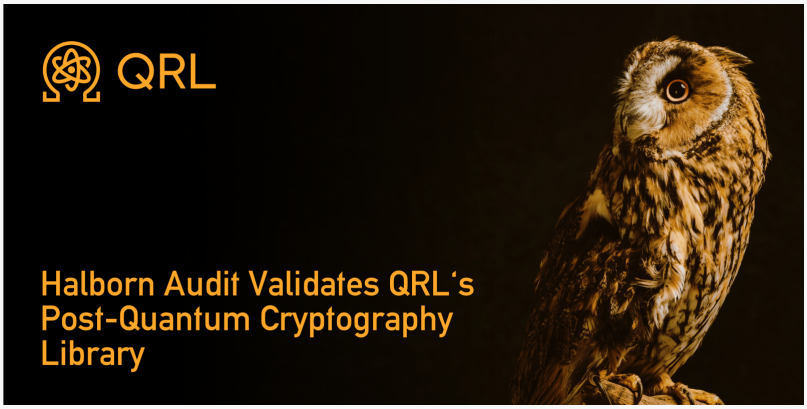
Halborn Audit Validates QRL's Post-Quantum Cryptography Library

Independent review finds no cryptographic vulnerabilities; all 13 findings rated Informational



ZUG, SWITZERLAND, April 3, 2026 /EINPresswire.com/ -- The Quantum Resistant Ledger (QRL) released the results of an independent security audit of its post-quantum cryptography library, conducted by blockchain security firm, and security partner, Halborn. The audit found no cryptographic vulnerabilities. All 13 findings were rated Informational, the lowest severity level, and the core signing, verification and key generation logic was validated as correct. All findings have since been resolved through code fixes or formal documentation.

The audit covers the two post-quantum digital signature packages at the heart of QRL's network, both implementing signature schemes approved by the National Institute of Standards and Technology (NIST) as part of its post-quantum cryptography standardization process.

The validated packages address a structural vulnerability present in most existing blockchain infrastructure. The majority of public blockchain networks rely on elliptic curve cryptography (ECC), a public-key scheme that a cryptographically relevant quantum computer (CRQC) could compromise, putting more than $2 trillion in digital assets at risk. That timeline has grown more concrete in recent years. Google's Willow processor demonstrated below-threshold quantum error correction in December 2024, IonQ's published roadmap projects a CRQC as early as 2028, and a Google research paper published March 30, 2026, warned that cryptographic migrations need to begin without delay while highlighting QRL as a presently post-quantum secure blockchain. Asset managers including BlackRock have flagged quantum computing as a material security risk to Bitcoin.

The Halborn audit is the latest in a series of third-party reviews of QRL's architecture. QRL's 1.x network launched in 2018 with post-quantum cryptography as a foundational design requirement and was externally audited by X41 D-sec and Red4sec, among the earliest public

blockchain networks to undergo such review at launch. QRL 2.0 extends that posture by incorporating quantum-safe smart contracts, a proof-of-stake consensus layer and continued third-party security audits from qualified firms.

"We have successfully completed our security assessment of QRL's post-quantum cryptography library. The fact that all findings were classified as informational highlights the project's strong security posture. Collaboration throughout the engagement was seamless, with the QRL team demonstrating responsiveness and efficiency in addressing all observations. We are happy to support their initiative to advance toward a quantum-secure future." - Gabi Urrutia, SVP Security & Field CISO at Halborn

The full audit report is available on the Halborn website. Previous QRL security audits are accessible in the QRL GitHub repository.

About The Quantum Resistant Ledger

QRL 2.0 is a proof-of-stake blockchain built with NIST-approved post-quantum cryptography from its initial launch. The network supports EVM-friendly smart contracts, NFTs and digital identities through the QRVM and the Hyperion smart contract language. More information is available at www.theqrl.org.

About Halborn

Halborn is the industry-leading blockchain solutions firm for enterprise-grade digital assets, trusted by the top financial institutions and blockchain ecosystem leaders. Experience world-class, end-to-end security, from smart contract auditing and pen testing to advisory services and beyond.

Media Contact

Jack Matier
Quantum Resistant Ledger
press@theqrl.org
