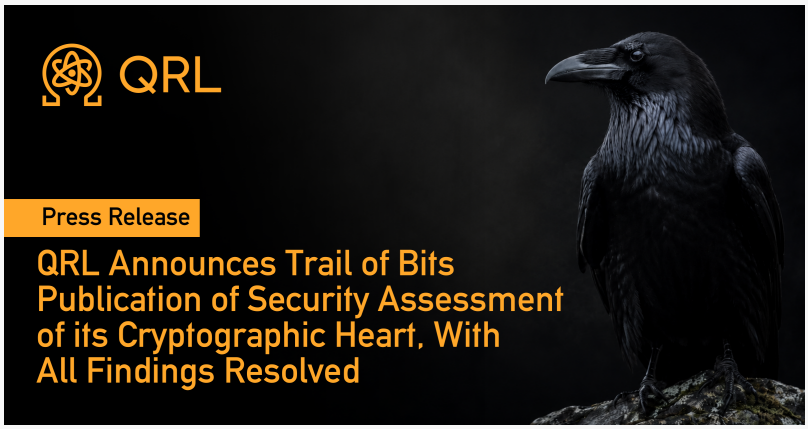
QRL Announces Trail of Bits Publication of Security Assessment of its Cryptographic Heart, With All Findings Resolved

An independent review examined the cryptographic heart of QRL, including implementations, public API, and wallet state management.



ZUG, SWITZERLAND, August 4, 2026 /EINPresswire.com/ -- The Quantum Resistant Ledger (QRL) today announced that Trail of Bits has published its independent security assessment of its cryptographic heart, go-qrllib, a cryptographic library being developed for QRL 2.0. The assessment identified 15 findings, one High, four Low, and ten Informational, all resolved following remediation by QRL and review by Trail of Bits.

The publication marks a security milestone for QRL 2.0, a post-quantum, EVM-friendly Layer-1 blockchain addressing the risk a cryptographically relevant quantum computer (CRQC) poses to public-key signatures used by blockchains.

Digital assets depend on these signatures to establish control and authorize transactions. A capable fault-tolerant quantum computer could use Shor's algorithm to recover private keys from public keys and forge signatures. A [March 2026 study](https://arxiv.org/abs/2603.28846) estimated that attacking secp256k1 could require about 1,200-1,450 logical qubits, while IBM, Quantinuum, and Microsoft target fault-tolerant or scalable systems by 2029. These roadmaps do not establish a CRQC date, but reinforce NIST's guidance to begin post-quantum migration now.

A three-consultant Trail of Bits team conducted an extensive review focused on go-qrllib's XMSS and ML-DSA implementations, exported API boundary, and wallet state-management paths. The work combined manual source review with fuzzing, external test vectors, reference-implementation comparisons, mutation testing, and other static and dynamic techniques.

Trail of Bits described the codebase as well-organized and modular, noted that its cryptographic

primitives strongly followed their specifications, and reported strong testing coverage and defensive wallet implementation. The findings primarily concerned the robustness of the library's exported API and supporting controls rather than the correctness of its underlying cryptographic primitives.

"go-qrllib is a well-organized, modular codebase with cryptographic primitives that closely follow their specifications. The QRL team was responsive throughout the engagement and resolved every finding we reported," said Filipe Casal, Principal Security Engineer at Trail of Bits.

QRL's remediation included stronger API validation; improvements to error handling, documentation, secret-memory handling, and wallet behavior; expanded regression testing; hedged ML-DSA signing by default; and additional CI/CD controls. Trail of Bits reviewed the fixes and mitigations on June 22, 2026.

Trail of Bits published the full assessment through its official Publications channel.

The source code is available in the go-qrllib repository.

About QRL

The Quantum Resistant Ledger is a public blockchain platform designed to address current cryptographic attacks and future threats posed by quantum computers. Development began in 2016, and QRL launched its first mainnet in 2018. QRL 2.0 is being developed as a post-quantum, EVM-friendly Layer-1 network featuring smart-contract functionality and a proof-of-stake consensus layer.

About Trail of Bits

Trail of Bits is a security research and engineering firm that has worked with Microsoft, Google, Meta, Adobe, and The Linux Foundation. It developed Slither and Manticore and has published open-source implementations of NIST-standardized ML-DSA algorithms.

Jack Matier
Quantum Resistant Ledger
email us here