EINPRESSWIRE

CycleCore Technologies Achieves Sub-100-Microsecond Post-Quantum Signing for Crypto Wallets and Cross-Chain Bridges

Real-time quantum-resistant signing and encryption at speeds invisible to end users, running on commodity hardware available today.

CycleCore Technologies - Real-time post-quantum cryptography for edge and safety-critical environments.

CASPER, WY, UNITED STATES, February 18, 2026 /EINPresswire.com/ -- CycleCore Technologies announced today that it has achieved real-time post-quantum cryptographic operations on commodity hardware, with independently measurable benchmarks confirming sub-100 microsecond signing for cryptocurrency wallets and sub-2 microsecond per-message encryption for cross-chain bridge communications.

The benchmarks, completed February 17, 2026 using NIST-standardized algorithms, demonstrate that quantum-resistant security can be deployed today without adding perceptible delay to transactions, attestations, or device communications.

> “Post-quantum security has been treated as a future problem. It is not. There is no longer a performance excuse for delaying adoption.”
>
> *CycleCore Technologies*

--Key Results--

CycleCore's benchmarks cover five critical areas of post-quantum performance.

Combined cryptocurrency wallet signing and verification completes in 98 microseconds, fast enough that users experience zero perceptible delay when approving transactions. The system supports both software and hardware wallet architectures, allowing exchanges and custodians to protect assets against future quantum threats without redesigning their existing infrastructure.

Cross-chain bridge encryption operates at 1.5 microseconds per message, representing negligible overhead compared to blockchain finality times measured in seconds. This protects high-value bridge communications against harvest-now-decrypt-later attacks, where adversaries capture encrypted traffic today with the intent of decrypting it once quantum computers reach sufficient capability.

Decentralized exchange order attestation completes in 94 microseconds, providing quantum-resistant proof of order submission timing suitable for regulatory compliance and dispute resolution. This enables exchanges to maintain verifiable, tamper-evident records of trade execution that will remain cryptographically valid in a post-quantum world.

A hybrid post-quantum handshake combining classical and quantum-resistant key exchange completes in 250 microseconds for Bluetooth Low Energy applications, adding only 77 microseconds of overhead compared to classical-only handshakes. This opens the door to quantum-resistant communications for edge devices, IoT sensors, and robotics operating in environments where low latency is critical.

Finally, a tamper-evident attestation chain adds each cryptographically signed entry in 72 microseconds, with full verification of a 100-entry chain completing in approximately 3 milliseconds. These audit logs are suitable for regulatory, insurance, and compliance verification across industries that require provable records.

This technology is particularly relevant to safety-critical fields such as cryptocurrency infrastructure, robotics, medical devices, and industrial automation.

"Post-quantum security has been treated as a future problem. It is not," said a spokesperson for CycleCore Technologies. "These benchmarks prove that quantum-resistant cryptography can run at speeds indistinguishable from classical systems on hardware available today. There is no longer a performance excuse for delaying adoption."

--Why It Matters--

The National Institute of Standards and Technology finalized post-quantum cryptographic standards in 2024, and government mandates are now pushing migration timelines into 2026 and beyond. Cross-chain bridges collectively hold billions of dollars in value and remain among the most attractive targets for harvest-now-decrypt-later strategies. Meanwhile, the broader cryptocurrency ecosystem faces an accelerating timeline as quantum computing research advances and early fault-tolerant systems come online.

CycleCore's approach delivers protection on existing hardware at speeds that do not impact user experience or system performance. Rather than requiring organizations to choose between security and speed, the technology eliminates the tradeoff entirely.

--About CycleCore Technologies--

CycleCore Technologies develops deterministic AI inference, agent infrastructure, developer tools, and security research for edge and safety-critical environments.

CycleCore Technologies
CycleCore Technologies
+1 307-215-3193
hi@cyclecore.ai