Post-Quantum

Cryptography Conference

Beyond the Quantum Threat: Demonstrating Real-World Blockchain Resilience

William Gee

Senior Advisor to 01 Quantum Inc. and Vice Chair of Asia PKI Consortium

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

01™ QUANTUM

Safeguarding **Crypto** against **quantum attacks.**

We are 01 Quantum from Canada

William Gee
Senior Advisor
01 Quantum (TSXV: ONE)

01 Quantum (TSXV:ONE)

Canadian publicly listed enterprise level cybersecurity provider

- Decades of experience in cybersecurity
- 15+ years of research
- Offers web2 post-quantum cybersecurity solutions
- US patents in post-quantum cryptography applications

Just in:
Latest patent-pending Quantum Crypto Wrapper (QCW) technology

Business partners:
HITACHI CGI THALES

Q-Day fast Approaching

Google
Quantum Echoes: step towards real-world applications

IBM 2025-2029 Deliveries
Loon (2025) → Kookaburra (2026) → Full fault-tolerant (2029)

Quantinuum (Honeywell)
New version within 2025 will be 1 billion times faster

Microsoft
"Majorana 1" topological core in Feb 2025

Google
Willow achieved a major breakthrough in Dec 2024

PROBLEM +

Your crypto **will** be exposed

$4T crypto assets at risk

Timeline to prepare:
before 2028

2025 changed everything:

"20% chance of quantum computers breaking modern cryptography before 2030"

Vitalik Buterin
Founder, Ethereum
(August 2025)

"All people alive will move Bitcoin into new quantum resistant addresses"

Paolo Ardoino
Founder, Tether
(February 2025)

01 QUANTUM

TECHNOLOGY +

Post-Quantum Cryptography (PQC)

PQC: cryptographic algorithms designed to be secure against quantum computers

Big tech is preparing for Q-Day:

Own quantum-resistant encryption protocol PQ3, March 2024

Google

Quantum-safe digital signatures in its Cloud Key Management. 2025

Microsoft

Early-access post-quantum cryptography tools for Windows and Linux, May 2025

Challenges for virtual assets...

Large signature & public key size

10x–100x larger than ECDSA

Breaks blockchain limits

Exceeds the data structure of the tx and gas constraints

Heavy verification

Slows down nodes and smart contracts

Incompatible formats

Not supported by current wallet/address systems

Hard fork ahead?

Bitcoin QRAMP + BIP 360

Ethereum Merge > Surge > Verge > Purge > **Splurge**

IMPORTANT +

Two major threat vectors:

- **“harvest now, decrypt later”**
- “trust now, forge later”

Reference:
https://bip360.org/
https://groups.google.com/g/bitcoindev/c/8PM6iZCeDMc
https://cryptoslate.com/vitalik-proposes-lean-ethereum-to-achieve-quantum-security-simpler-validator-operations/
https://vitalik.eth.limo/general/2024/10/29/futures6.html

01 QUANTUM

Ways to solve Post-Quantum Cryptography (PQC) challenge in crypto

NOTE +

Theoretically Hybrid Classical + PQC works on existing L1s, but the signature size make it practically not possible to implement

Approach	Adoption Ready	Works on Existing L1s	Decentralized	Convenient UX
New PQC L1 Blockchains	-	-	+	-
PQC Bridges	+	+	-	-
qLABS Quantum-Resistant ZK Verification Protocol	+	+	+	+

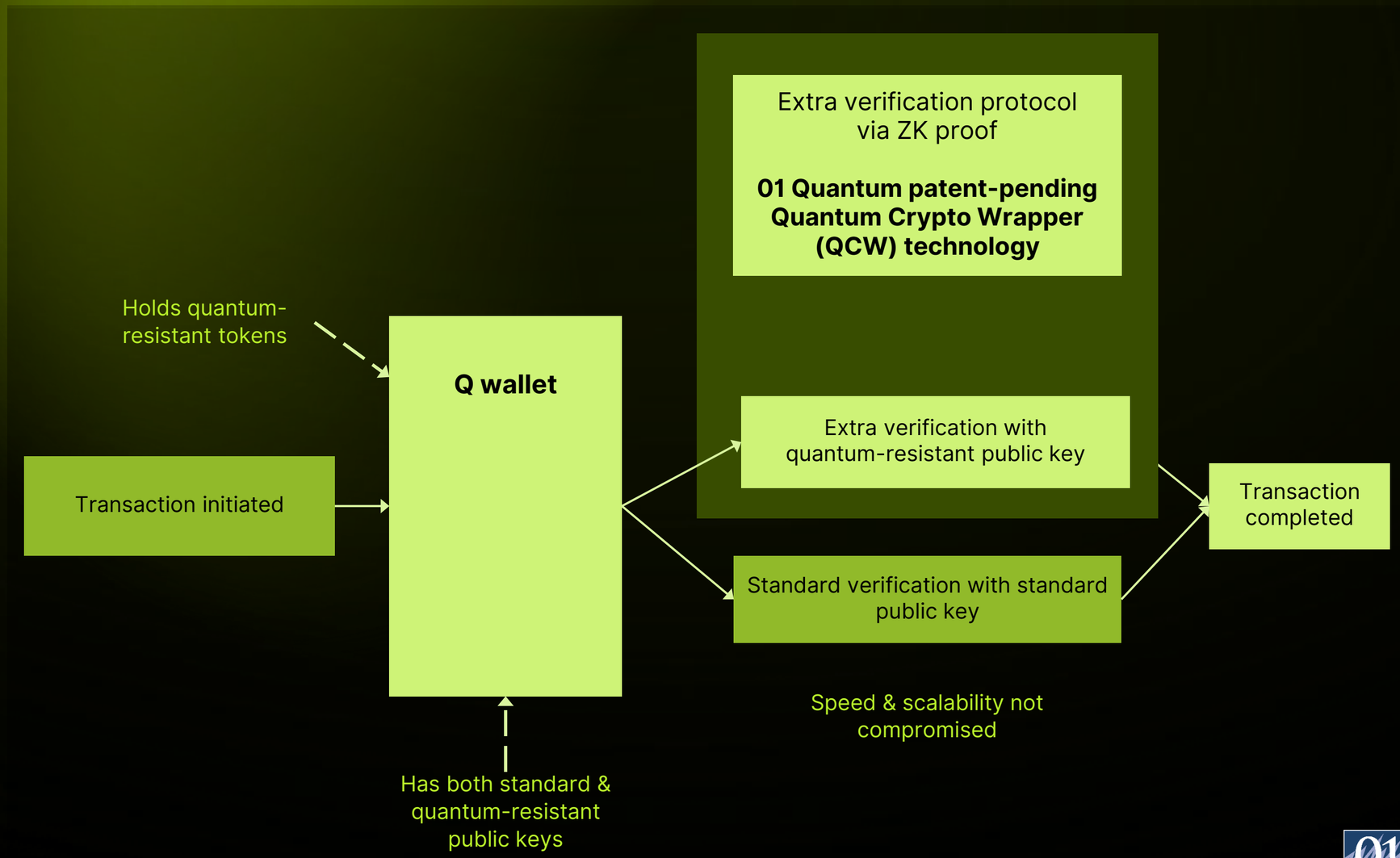
Addressing the $4T problem for virtual assets

Built on IronCAP™, a NIST-approved post-quantum technology by 01 Quantum, qLABS applies **NIST-approved cryptography** and **zero-knowledge proofs** to verify quantum signatures on legacy chains.

How did we get here?

2018	Core tech IronCAPTM launched
2022	US Patent: 11,271,715 granted
2022-now:	Research on post-quantum cryptography application for blockchain
2023-2024	Quantum-verification protocol POC on Solana successfully implemented
2024	US Patent: 11,669,833 granted
2025 May	Quantum-verification protocol POC tech audit completed
2025 June	Patent US patent-pending 63/832,787

*National Institute of Standards and Technology, US



Broader issues

Smart Contracts

Practicality and complexity of migrating to upgradeable smart contracts

Layer 2s

Integrity of L2 off-chain computations and state transitions must also be made quantum-resistant

Wallets and Remapping

Legacy on-chain records become invalid with change of wallet addresses

Irrecoverable Asset

Dormant and lost wallets giving rise to ethical and economic challenges posed by PQC migration

Take-away
Path to Quantum-safe virtual assets

Technical Whitepaper

Q4 2025-Q1 2026 +

- **Quantum-Resistant ZK Verification Protocol:**
  uniting post-quantum cryptography with zero-knowledge proofs for quantum-safety on **Hyperliquid**
- **Q-resistant Wallet:**
  quantum-resistant wallet + API & SDK for integrations
- **Q-resistant Token:**
  quantum-resistant token on **Hyperliquid** for forever safe transactions
- **Bridge infrastructure for $HYPE wrapping:**
  making **$HYPE** token quantum-resistant

Q2 2026 - Q1 2027 +

- **Premium wallet features & Institutional Vaults:**
  multisig, automated payments, institutional grade security
- **Quantum-resistant Token Generator SDK:**
  enabling everyone to launch their own quantum-resistant token on **Hyperliquid**
- **Quantum-resistant stablecoin infrastructure:**
  quantum-resistant stablecoins on **Hyperliquid**

Q1 QUANTUM

01 QUANTUM™

Safeguarding **Crypto** against **quantum attacks.**

Thank You!

William Gee
Senior Advisor