Quantum Computing poses a credible near-term threat to the security of Bitcoin

The Quantum Computer threat – to Bitcoin, Ethereum, and elliptic curve cryptography – and the role of a Quantum Resistant Ledger in safeguarding decentralized digital assets and communications

“… to avoid that failure of nerve for which history exacts so merciless a penalty — we must have the courage to follow all technical extrapolations to their logical conclusion.” — Arthur C. Clarke

Summary

Quantum Computers pose a credible threat to the elliptic curve cryptography (ECDSA) used by Bitcoin and Ethereum for asset security, and mitigation of this threat will not be simple or fast even if urgently prioritized. Quantum Computing progress (in terms of error correction / hardware quality / algorithmic advances) is happening at a faster rate than predicted by almost anyone, and could threaten the security model of (and trust in) today’s largest public blockchains in the next 1-5 years.

Major centralized entities and platforms (such as Microsoft, Google, iMessage, Zoom, and Cloudflare) have already begun transitioning to post-quantum cryptography, and in some cases are already finished. **Despite the US Government phasing out current public-key algorithms from National Security Systems starting in 2025, there is still no major cryptocurrency exchange that allows its users to hedge against quantum risk via quantum-secure digital assets.** Lack of exchange support for the open-source Quantum Resistant Ledger (QRL) hampers adoption by end-users and other applications that could benefit from QRL’s cryptographic toolkit. By integrating QRL, exchanges would enable users to protect some portion of their assets against quantum risk while accelerating discourse about the urgency of proactively protecting Bitcoin and Ethereum.

Without urgent action, it appears increasingly plausible that the cryptocurrency industry will be caught off-guard by quantum computer progress just as digital assets begin to go mainstream in the form of RWAs and tokenized financial instruments.

The Quantum Resistant Ledger (QRL) has implemented the world’s first (and currently only) fully quantum-resistant blockchain platform, open-source and live for 7+ years, using a post-quantum signature standard (XMSS) selected by NIST. QRL has supported pioneering research on post-quantum signature aggregation and was referenced as a building block in a Lockheed Martin patent for military-grade post-quantum communication techniques. QRL is also a member of the Linux Foundation’s Post-Quantum Cryptography Alliance.

Contents

The Quantum Computer Threat to Bitcoin, Ethereum, and ECDSA

1. Shor's Algorithm and ECDSA Vulnerability

- **Exponential Speedup for Discrete Logarithms: Shor's algorithm can factor large integers and solve discrete log problems in polynomial time, breaking ECDSA**
- **Bitcoin:**
  - ~33% of BTC linked to exposed public keys (e.g., pre-2012 P2PK – "pay-to-public-key" – mining rewards, reused addresses)
  - ~2500 logical qubits to derive private keys for secp256k1
- **Ethereum:**
  - Account-based model reuses addresses, exposing public keys permanently
  - Deloitte estimates ~65% of Ether is held in quantum-vulnerable addresses

Attack Modes

1. **Storage Attack (Long-Range Attack):**
   - Adversary locates addresses with known public keys, uses Shor's algorithm to derive private keys at leisure, and transfers the funds.
2. **Transit Attack (Short-Range Attack):**
   - When a transaction broadcasts a public key, a quantum adversary factors it before transaction confirms, then re-signs with a higher fee to steal the funds. *If no PQC upgrade before this attack is possible, upgrade becomes impossible for any wallets without EdDSA possibility of retroactive ZK seed-phrase proof*

2. Grover's Algorithm and Mining

- **Quadratic Speedup in Search:** Grover's algorithm reduces brute-force search (in SHA-256 or similar hash functions) from 2^256 to 2^128
- **Impact on PoW:**
  - Could shift mining advantage to quantum-equipped entities, potentially causing more frequent blockchain forks or consensus disruptions.
  - Less critical than Shor's threat, still a potential security/stability concern.

3. Proposed Mitigations

- **Bitcoin:** BIP-360 (now reduced scope) / BIP-420 / Commit-Delay-Reveal / Hourglass v1 and v2 / QR Migration BIP (Lopp et al)
- **Ethereum:** Commit–delay–reveal, "rescue" hard-forks, or hybrid signature schemes.
- **EdDSA Chains** (Sui, Solana, Cosmos, Near, …) actually have a partial escape-hatch
- **Challenges:**
  - Large-scale transitions require consensus among miners, developers, and participation from *all users* by deadline (at risk of coins being burned)
  - Lost / inactive addresses complicate "forced migration" to PQ keys
  - PQ sigs 10x larger, migration could require extreme congestion or downtime

4. Expert Opinion / Social Proof

- Zooko / Scott Aaronson (**Shor's Risk by 2028**) / Vitalik (**Shor's Risk by 2028**) / Jameson Lopp / Deloitte / Alex Pruden (P11)

5. Common Misconceptions

- **"SHA-256 won't be broken…"**
  - While true that SHA-256 (used in Bitcoin's POW) is not "broken" by quantum algorithms, this ignores the real issue: Shor's algorithm can break ECDSA-based public–private key cryptography, enabling key theft and unauthorized spending. The security of most funds on Bitcoin and Ethereum depends on discrete logarithm hardness, not on SHA-256 alone.

- **"We'll have bigger problems… / bank accounts will get hacked first…"**
  - A common argument is that if quantum computers can break ECDSA, the entire internet is in trouble anyway. However, web2 systems can more easily schedule downtime or be centrally updated to post-quantum cryptography – and in many cases *already have*. Decentralized blockchains do not have that luxury: any fork or signature scheme change requires widespread consensus, and it must happen before any large-scale quantum attack occurs.

- **"Bitcoin will just transition to PQ sigs…"**
  - Switching Bitcoin or Ethereum to post-quantum signatures is not trivial. It involves:
    - **Technical complexity:** Next-generation post-quantum schemes often have larger keys/signatures and untested performance implications.
    - **Governance hurdles:** Hard forks require community consensus, and any missed or lost addresses complicate transitions. A rushed upgrade could be extremely contentious and disruptive. *Will Satoshi's coins be burned or stolen by a quantum computer attacker?*

- **"My Bitcoin will be secure…"**
  - Some users argue that if they never reuse an address or rely on the "pay-to-public-key-hash" structure, they are safe. While locally true, in reality:
    - Locally "safe" coins lose value if a large-scale quantum attack destabilizes the network globally (e.g., by stealing or dumping significant amounts of BTC).
    - Satoshi's early coins (and others) used pay-to-public-key (P2PK) addresses before 2012, leaving millions of BTC potentially at risk.
    - Approximately ~33% of Bitcoin in circulation resides in addresses whose public keys have already been exposed, making them vulnerable to a quantum adversary.

Quantum Computer Progress (Algorithms, Hardware, Error Rates, Logical Qubits)

Below is a condensed overview of recent progress impacting the timeline and feasibility of breaking elliptic curve cryptography (ECDSA) via quantum computation.

Resource: Quantum Difficulty of various applications (ECC break before RSA or chemistry)

---

1. Algorithmic Advances

(a) "How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates"

(arXiv:2306.08585) Shows a refined approach for Shor-like circuits factoring elliptic-curve keys with fewer gates, achieving up to a 5x reduction in Toffoli count. Demonstrates that with improved architecture (6k modules, each 1152 qubits, 10^-3 error rate), a 256-bit ECC key can be derived in ~10 minutes. Implies faster attacks against ECC than older resource estimates.

~~**(b) "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits"**~~

(arXiv:1905.09749) Shows that Shor-based factoring of 2048-bit RSA could be done with ~20 million physical qubits (error rates ~10^-3), producing a factorization in under a day. While RSA ≠ ECC, it confirms the feasibility of large-scale discrete-log attacks once hardware scales.

(b) "How to factor 2048 bit RSA integers with less than a million noisy qubits"

(arXiv:2505.15917) An improvement over the prior SOTA by same authors, reducing number of qubits needed by 20x

(c) "Factoring integers with sublinear resources on a superconducting quantum processor"

(arXiv:2212.12372) Demonstrates factoring up to 48-bit integers on a 10-qubit superconducting quantum device with sublinear circuit depth. Estimates ~372 physical qubits and moderate-depth circuits could challenge RSA-2048. Indicates that real hardware is moving beyond mere theory.

(d) "A Modular, Adaptive, and Scalable Quantum Factoring Algorithm"

(arXiv:2509.05010) Introduces a windowed formulation of Shor that keeps the counting/phase register to a few qubits per block (e.g., 3–4) while leaving the work register unchanged. Net effect: shallower circuits and lower concurrent-qubit/coherence burden without changing asymptotic complexity—complementary to arithmetic-layer optimizations.

---

2. Hardware & Error-Correction Breakthroughs

(a) "A manufacturable platform for photonic quantum computing"

(arXiv:2404.17570) Introduces a photonic chip fabrication process with ~99.98% single-qubit fidelity and ~99.2% two-qubit fidelity. Fiber-based interconnects enable modular scaling. In principle, fusion-based photonic systems could be extended to large qubit counts under fault-tolerance thresholds.

(b) "Active volume: An architecture for efficient fault-tolerant quantum computers…"

(arXiv:2211.15465) Describes a method for reducing idle-qubit overhead by leveraging non-local connections. This approach can drastically cut qubit requirements for Shor-like circuits, further accelerating the timetable for cryptographically relevant machines.

(c) "Quantum Error Correction of Qudits Beyond Break-even"

(arXiv:2409.15065) Demonstrates qudit-based error correction with improved lifetimes compared to physical qubit coherence times. Surpassing "break-even" indicates that large-scale, robust qudit codes may emerge sooner than expected, reducing logical qubit costs.

(d) "Logical computation demonstrated with a neutral atom quantum processor"

(arXiv:2411.11822) Presents multi-qubit logical operations on a 256-qubit neutral-atom device with repeated loss correction. High connectivity plus demonstrated error correction suggests neutral-atom architectures are a viable path toward 2k–3k logical qubits needed to break ECC.

(e) "Scaling and logic in the color code on a superconducting quantum processor"

(arXiv:2412.14256**;** Google**;** Nature**)** Demonstrates logical error suppression when scaling the color code from distance-3 to -5 ($\Lambda_{3/5} \approx 1.56$), low-overhead transversal Clifford gates (≈0.27% added error), >99% magic-state injection fidelity with ~75% post-selection retention, and logical-state teleportation via lattice surgery (≈86.5–90.7% fidelity). Establishes color codes as a viable path to fault-tolerant logic on superconducting hardware.

(f) "Room-temperature valley-selective emission in Si–$MoSe_2$ heterostructures enabled by high-quality-factor chiroptical cavities"

Demonstrates a silicon chiral metasurface coupled to a monolayer $MoSe_2$ that achieves room-temperature valley-selective emission with chiroptical cavity Q-factors up to ~450 and a record degree of circular polarization ≈0.5, boosting valley-specific radiative rates by ~13×. By entangling photon spin with electron valley pseudospin on a CMOS-compatible chip without cryogenics, it points toward ultracompact, mass-manufacturable quantum light sources and on-chip quantum communication hardware—further eroding "dilution fridge" as a barrier to scaled quantum networks.

---

3. Breaking Encryption: RSA & ECC

(a) "Quantum inspired factorization up to 100-bit RSA number in polynomial time"

(arXiv:2410.16355) Shows factoring of 100-bit RSA keys via novel quantum-inspired classical algorithms. Although scaling remains polynomially high, underscores urgency of adopting post-quantum schemes.

(b) "Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126133 Cat Qubits"

(arXiv:2302.06639) Shows discrete-log solutions for 256-bit ECC in ~9 hours on ~10^5 error-corrected qubits (cat-state approach). Reinforces that ECC-based crypto can be compromised once large cat qubit arrays emerge.

(c) "Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms"

(arXiv:2404.16450) Provides rigorous proofs for new Shor-like algorithmic variants (e.g., Regev) with fewer gates. Validates a path to more efficient factoring/discrete-log circuits, pushing practical ECC breaks closer.

(d) "Brace for impact: ECDLP challenges for quantum cryptanalysis"

(arXiv:2508.14011) Under explicit, testable assumptions, places full 256-bit ECDLP in a 2027–2033 feasibility window—arguing for proactive migration to post-quantum signatures.

(e) "Breaking a 6-Bit Elliptic Curve Key on IBM's 133-Qubit QPU"

(Twitter thread) Steve Tippeconnic demonstrates a Shor-style ECDLP toy break on real hardware—recovering k = 42 for a 6-bit key on ibm_torino with a deep (~340k-layer) circuit; illustrates the interference ridge over a 64×64 output grid. Symbolic progress toward scalable ECC attacks, not a practical threat to ECC-256 yet.

---

4. "Logical Qubits" Milestones and Public Claims

- **Harvard & QuEra**: Performed 48-logical-qubit circuits
- **Quantinuum & Microsoft**: Achieved 12 low-error logical qubits
- **Public Roadmaps foresee 10,000 - 1M+ physical (100-1000+ logical) qubit fault-tolerant systems by 2030** (Nevin's Law implies it could go faster)
    - Shift from monolithic to networked hardware is crucial for scale
- IonQ publicly predicts RSA-2048 and ECC-256 will be broken in a "few years" or sooner
- Alice & Bob achieve superconducting qubit stability benchmark 5 years early
- **Neutral Atom qubit growth rate puts CRQC (Bitcoin Killer) ~18 months away**

US Government PQ-Cryptography Transition

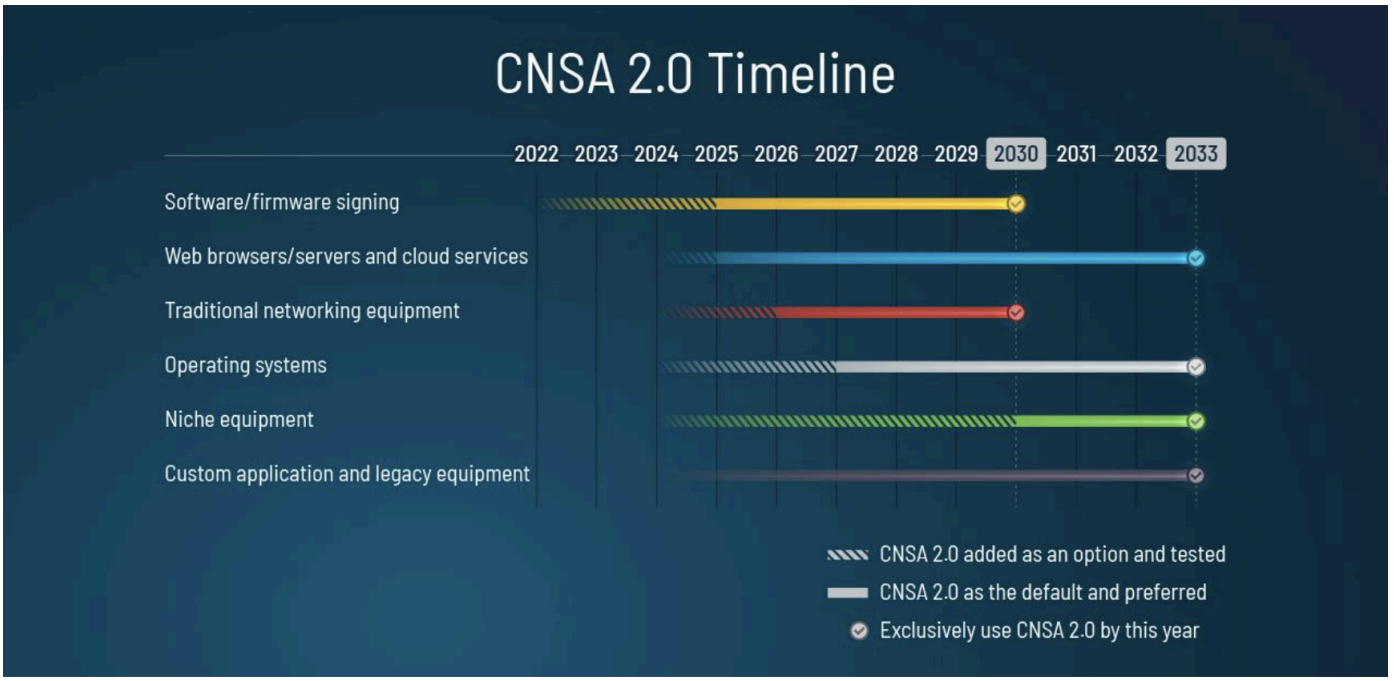
U.S. federal guidance mandates phasing out classical elliptic curve cryptography (ECC) before quantum computers become cryptographically relevant. Below is a condensed overview with a table highlighting transition deadlines published by agencies such as NSA, NIST, CNSS, and OMB.

Notable: Canada and EU also have PQC upgrade plans with critical systems requiring protection by 2026 and 2030 overall cutoff

---

Key Milestones

- **National Security Memorandum 10 (NSM-10):** Sets 2035 as the target for completing migration to quantum-safe algorithms in National Security Systems (NSS).
- **CNSA Suite 2.0 (NSA):** Removes purely classical ECDH/ECDSA from future NSS encryption and signatures, urging early PQC readiness as soon as 2025 for new acquisitions.
- **NIST SP 800-131A (to be updated):** Anticipates deprecating all ECC at ≥ 128-bit security by 2030–2035; 112-bit curves or lower are disallowed sooner.
- **OMB Memo M-23-02 (November 2022):** Directs civilian agencies to inventory ECC-based systems and prioritize post-quantum adoption, especially for data sensitive beyond 2030.



Practical Notes

1. **“Store-Now, Decrypt-Later” Risk**
   Government guidance stresses that adversaries may record ECC-encrypted data now and break it once large quantum computers exist. Agencies must mitigate this risk by acting before 2030–2035.

2. **Immediate Next Steps**
   - By 2025: No purely ECC-based designs in new NSS acquisitions (NSA/CNSA 2.0).
   - Inventory existing ECC usage (OMB M-23-02).
   - Plan to integrate NIST-approved quantum-safe schemes (e.g., CRYSTALS-Kyber for key exchange, Dilithium or hash-based signatures for authentication).
3. **Software & Hardware Upgrades**
   Most transitions require updating HSM firmware, cryptographic libraries, and PKI. The government urges agencies and contractors to embrace “crypto agility” to ease future PQC updates.

2025 marks the first critical cutoff for avoiding new ECC-only deployments in certain U.S. government systems, and 2035 is the final “drop-dead” date for ECC in National Security contexts. By then, post-quantum cryptography will be mandatory for both classified and sensitive unclassified data.

References and URLs

- The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

- OMB Memo M-23-02 – *Migrating to Post-Quantum Cryptography (Nov 2022)*

- NIST IR 8547 (Initial Public Draft) – *Transition to Post-Quantum Cryptography Standards (Nov 2024)*

Web2 Giants Already Transitioning to PQ-Security

Technology giants like Microsoft and Amazon have accelerated their transitions to PQC. This shift underscores that large-scale deployment is feasible with centralized infrastructure and somewhat urgent already, especially for "harvest now, decrypt later" attacks

---

1. iMessage (Apple)

In February 2024, Apple announced "iMessage with PQ3," introducing post-quantum cryptography (Kyber-based key exchange + periodic PQ rekeys) for all iMessage traffic on iOS 17.4 and above. Apple's PQ3 protocol uses hybrid ECDH + Kyber to protect against a "harvest-now, decrypt-later" attack. Engineers estimate that all iMessage conversations between PQ3-capable devices are now fully quantum-safe by default.

---

2. Cloudflare

Starting in 2018, Cloudflare led a series of experiments (CECPQ2, CECPQ2b) combining classical key agreements (X25519) with PQC (NTRU, SIKE). In 2023–2024, Cloudflare reported that ~2% of TLS 1.3 connections globally used a post-quantum (Kyber) hybrid, primarily driven by Chrome's partial rollout. Cloudflare servers also offer post-quantum origin connections for website owners, though some fraction (~0.34%) remain incompatible.

---

3. Zoom

In May 2024, Zoom announced "post-quantum E2EE" for Zoom Meetings. The new E2EE uses Kyber-768 for ephemeral session key encryption and is available to all Zoom Workplace customers. Zoom's approach mitigates "harvest now, decrypt later" eavesdropping on video conferences, making Zoom one of the first UCaaS providers with default post-quantum protections for real-time media.

---

4. Chrome

Google reported in August 2024 that Chrome had enabled "ML-KEM by default for TLS 1.3 and QUIC on desktop" in an experimental capacity, impacting tens of millions of daily users. As of Q3 2024, ~10% of Chrome desktop connections to Google services use post-quantum key agreement. Google engineers note that large-scale deployment is constrained by legacy network appliances but foresee "double-digit adoption" of PQ key exchange in the short term.

**This document was not produced or approved by The QRL Foundation or anyone associated with The QRL Foundation (Author: Charlie Thompson)*

The Quantum Resistant Ledger: Facts and History

- **Earliest XMSS Adoption:** QRL launched **mainnet in 2018** with **XMSS**—a hash-based signature scheme later recommended by NIST SP 800-208—in collaboration with recognized post-quantum cryptographers. This provides **quantum-resistant addresses** at the protocol level

- **Open Source & Community-Driven:** QRL's code (node software, ephemeral messaging, multi-sig, etc.) is fully MIT-licensed on GitHub. Security audits by Red4Sec and x41 D-Sec attest to QRL's focus on reliability. A post-quantum ephemeral messaging layer supports post-quantum private communication. Existing tooling includes a block explorer, a web wallet (with document notarization and message signing / verification functions) and a Ledger Hardware Wallet Integration

- **Lockheed Martin Patent:** "Quantum Resistant Ledger for Secure Communications" (US 20240048369 A1) references QRL as the underlying network for post-quantum decentralized communications techniques —signaling adoption by government-adjacent professional developers

- **Research & Signature Aggregation:** QRL solicits and funds advanced cryptographic research, including through Geometry Labs creators of the *lattice-algebra* library. Their "Fusion" pq-signature aggregation research aims to improve scalability and speed (of PoS, STARKS, …) in quantum-safe cryptography

- **Regulatory Hurdles & Delisting:** In **2019**, QRL was removed from Bittrex due to uncertainty about digital asset regulations. It continues trading on other markets globally, but none which allow US citizens to trade at serious volumes without major price impact

- **EVM-Compatible Upgrade (Zond):** with second testnet arriving Q1 2025, "Zond" merges QRL's quantum resistance with EVM-compatible smart contracts. Developers will be able to migrate/deploy stablecoins, dApps, and custom tokens written in Solidity while benefiting from a **fully post-quantum** underlying ledger. Migration from XMSS to SPHINCS+ improves UX by removing need to use an OTS (One Time Signature) for each transaction and rotate wallets when user runs out of OTS keys, making integrations (for exchanges and other actors) much simpler

- **Industry Collaboration:** QRL is an active member of the Post-Quantum Cryptography Alliance, working alongside global experts on next-generation cryptography

Linux Foundation Post-Quantum Cryptography Alliance