EXPLAINER

Crypto and Quantum Computing

A sufficiently powerful quantum computer could one day challenge the cryptography that secures digital assets across major blockchains. Although these machines do not yet exist, there is broad expectation that they will eventually be built—and while many expert timelines point to at least a decade, shorter horizons cannot be ruled out.

The practical issue is that upgrading the security of decentralized systems—blockchains, wallets, exchanges, and hardware—takes time. The policy question, therefore, is how to begin a measured transition to quantum-resilient onchain finance now, rather than waiting until the need becomes urgent. That is why industry and academic experts, including those at Coinbase's Independent Advisory Board on Quantum Computing and Blockchain, are mobilizing around practical solutions, as explained in a detaild new position paper on quantum computing and blockchain that sets out threat scenarios and migration paths for crypto infrastructure.

How it Works

Most public blockchains, wallets, and exchanges rely on public-key cryptography to prove ownership and authorise transactions. Users share a public key (or a derived address) and keep their private key secret. Classical attackers cannot feasibly derive the private key from the public key; the search space is too large. Hash functions, used for commitments and proof-of-work, offer similar protection against tampering.

Large-scale quantum computers could change this balance. Shor's algorithm can efficiently solve the hard mathematical problems behind widely used public-key schemes, including RSA and elliptic-curve cryptography. With a cryptographically relevant quantum computer, an attacker could, in principle, derive a private key from its public counterpart and steal funds. Other quantum algorithms, like Grover's algorithm, can speed up brute-force search, modestly weakening some symmetric schemes and hash functions.

The immediate threat is limited—such quantum computers do not yet exist—but major changes to blockchains take a long time. Furthermore, once a blockchain has been updated to be quantum safe, users need to transfer all of their funds. Therefore, the time to begin the process is now.

The good news is that post-quantum cryptography (PQC)—new algorithms designed to resist known quantum attacks—has advanced quickly. Standard-setters like NIST are selecting lattice-based and hash-based schemes for digital signatures and key exchange. Other remaining challenges include integrating PQC into wallets, protocols, and validators; designing safe migration paths; and coordinating across chains and jurisdictions. Specifically, initiatives like Coinbase's Independent Advisory Board on Quantum Computing and Blockchain are bringing together leadingquantum and cryptography experts to analyse these issues for crypto specifically and to provide a roadmap for how exchanges, issuers, and developers can upgrade their systems over time.

Significance and Solutions

- **Safeguarding long-lived onchain value:** Crypto now secures stablecoins, tokenised treasuries, and long-horizon smart contracts. Without a PQC migration, a future quantum adversary could compromise assets that are expected to remain safe for decades.

- **Protecting vulnerable users:** Households and small firms in both advanced and emerging economies increasingly rely on crypto—especially stablecoins—for remittances, savings, and protection against inflation or capital controls. A poorly managed quantum transition would disproportionally harm these users if only large institutions can afford to upgrade early.

- **Maintaining financial stability and market integrity:** If validator keys, bridges, or large custodial wallets were compromised, attackers could disrupt settlement, manipulate markets, or trigger loss of confidence. Quantum-resilient designs for consensus keys and cross-chain infrastructure are therefore part of the financial-stability agenda.

- **Supporting public-sector and institutional adoption:** Governments and institutions exploring tokenised bonds, onchain settlement, and programmable benefits will only scale these projects if they are confident that the underlying cryptography remains secure in a quantum era.

Conclusion

With the right response, quantum computing's effects on crypto can be managed as a straightforward design consideration. Policymakers can support this transition by embedding crypto-agility into digital asset rules so systems can upgrade cryptography over time, and by aligning with post-quantum standards tailored to blockchain use cases such as wallets, validators, and cross-chain infrastructure.

They can also encourage transparency by asking major industry participants to publish quantum-risk assessments and migration plans, while supporting collaborative testing and expert groups to trial solutions in practice. Approached this way, the quantum era can reinforce the security and resilience of onchain financial infrastructure.