Bitcoin faces the quantum countdown

Over the past year, most of the market focused on bitcoin's price swings and investor sentiment. While debates over regulation, adoption, and inflation dominated headlines, a new challenge quietly emerged: the rise of quantum computing. Bitcoin recently dipped as markets weighed these potential risks, raising questions about the cryptocurrency's long-term security and resilience.

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Hugo Morel
Syz Research Lab Team
hugo.morel@syzgroup.com

Syz PRIVATE BANKING

Introduction

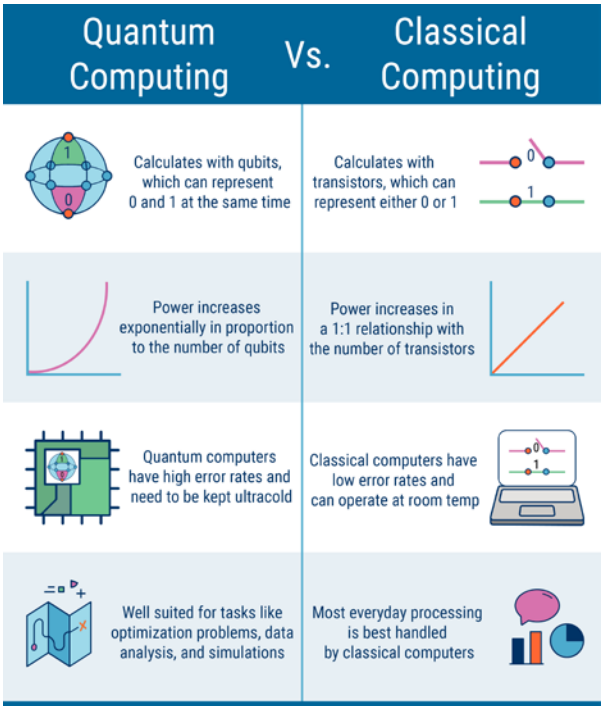
Quantum computing is advancing quickly and is raising new questions about the long-term security of blockchain systems. Because bitcoin relies on cryptography to secure transactions and ownership, researchers are examining whether future quantum computers could weaken or break these protections.

These concerns are not limited to academic research. Christopher Wood, global head of equity strategy at Jefferies, recently removed bitcoin from his model portfolio, citing the risk that advances in quantum computing could undermine its cryptographic foundations. He warned that any successful breach would challenge bitcoin's role as a long-term store of value.

The quantum computing threat

Quantum computing is often described as the next major step in computing technology. Unlike classical computers, which process information using bits that are either 0 or 1, quantum computers use quantum bits, or qubits. Qubits can represent multiple states at the same time thanks to a property known as superposition. Combined with other quantum effects such as entanglement and interference, this allows quantum computers to process certain types of problems far more efficiently than traditional machines.

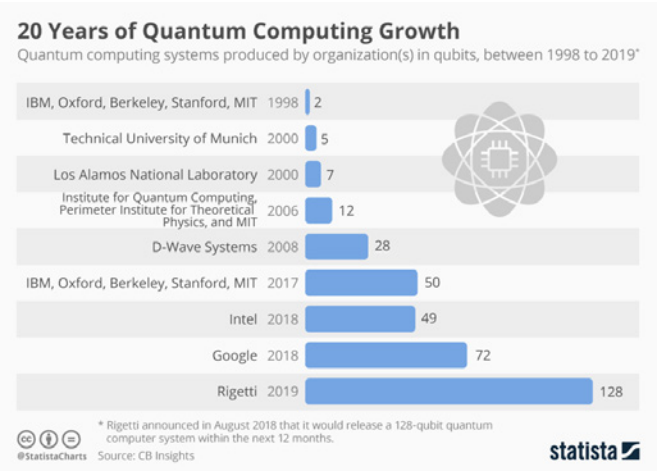
A simple analogy helps clarify the difference. Timothy Hollebeek, Industry Standards Strategist at DigiCert, compares classical computing to navigating a maze by trying one path at a time, while a quantum computer can explore all possible paths simultaneously. This parallel processing ability explains why quantum machines are particularly well suited to complex mathematical problems, such as factoring large numbers or identifying patterns in vast datasets.



Source: CBInsights

Recent advances illustrate this potential. Google's quantum chip, Willow, reportedly solved a specific computational problem in under five minutes—one that would take classical supercomputers an impractically long time. It is approximately 13,000x faster than the best supercomputers in the world. Results like this help explain why quantum computing attracts attention in fields such as medicine, logistics, and materials science.

Despite the excitement, quantum computing remains at an early stage of development. Today's machines face major technical constraints. Qubits are extremely fragile, require temperatures near absolute zero, and are highly sensitive to noise, which introduces errors. Even under controlled conditions, maintaining a stable quantum state for more than a brief moment is difficult. Google's Willow chip, for example, operates with 105 qubits, while practical, fault-tolerant systems would likely require thousands of stable, interconnected qubits.

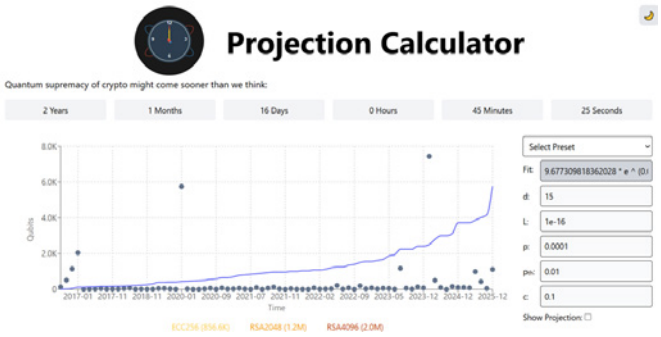


Source: Statista

The rise of quantum computing naturally raises questions about the long-term security of digital systems that rely on cryptography, including cryptocurrencies. Indeed, because bitcoin's design is based on mathematical assumptions about computational limits, any major shift in computing power invites closer examination.

The real threats that could cripple bitcoin's value

"Quantum computers are not a question of if, but when," notes Timothy Hollebeek, Industry Standards Strategist at DigiCert. This statement captures why technological advances like quantum computing are increasingly discussed as a potential long-term risk for bitcoin.



Source: Projection Calculator

The most serious concern involves Shor's Algorithm, a quantum algorithm capable of breaking the digital signature scheme (ECDSA) that bitcoin uses to prove ownership of funds. In today's classical computing environment, deriving a private key from a public key is effectively impossible. In a future where large-scale quantum computers exist, this could change. An attacker could, in theory, recover a private key from a public key in a relatively short time, allowing them to move funds without the owner's consent.

This risk is unevenly distributed across the bitcoin network. Approximately 25% of all bitcoins over 5mn BTC are stored in "vulnerable" addresses, including early P2PK addresses and any reused P2PKH addresses. This group also includes Satoshi Nakamoto's estimated 1.1 million BTC. These addresses are more exposed because their public keys are already visible on the blockchain, making them susceptible to quantum attacks. If a quantum attacker were able to move even a portion of these coins, the resulting supply shock could be catastrophic, severely undermining confidence in bitcoin's ownership model and putting strong downward pressure on its price.

Even newer address types are not entirely immune in extreme scenarios. One frequently discussed theoretical risk involves transactions waiting in the mempool—the pool of unconfirmed transactions broadcast to a blockchain's nodes. In this case, a sufficiently powerful quantum computer could observe a transaction before confirmation, derive the associated private key in real time, and broadcast a competing transaction that redirects the funds before the original one is finalised. While purely theoretical, this scenario highlights how speed advantages could matter as much as raw computing power.

Beyond direct theft, quantum computing could also undermine trust in bitcoin's fairness and privacy. Grover's Algorithm could give quantum-equipped miners a major advantage in proof-of-work mining, potentially leading to mining centralisation. If a single actor gained enough power, they could censor transactions or reorganise blocks, damaging bitcoin's reputation as a decentralised network.

Another concern is known as "harvest now, decrypt later", which is the act of collecting encrypted blockchain data today, with the expectation that future quantum machines could decrypt it. While this would not change past transactions, it could expose identities behind pseudonymous wallets or reveal historical information, weakening perceived privacy.

These technical concerns are increasingly reflected in market behaviour. As of early 2026, quantum-related risks have moved beyond theory and begun to influence investment decisions. Bitcoin, for example, underperformed gold by about 6.5% year-to-date, while gold gained around 55% over the same period. This shift pushed the bitcoin-to-gold ratio down to roughly 19BTC per ounce of gold, reflecting a more cautious market sentiment.

Bitcoin-to-gold ratio

Source: zerohedge

What "breaking" bitcoin would look like, and why it remains resilient

Right now, bitcoin relies on Elliptic Curve Cryptography (ECC), specifically the "secp256k1" curve, to generate public and private keys. This system uses ECDSA signatures to verify transactions, but powerful quantum computers could eventually break it, putting funds and transaction security at risk. A practical approach is adopting post-quantum cryptography (PQC), which provides quantum-resistant security. Networks can implement PQC gradually, replacing vulnerable algorithms over time rather than rebuilding the system from scratch.PQC would introduce a three-layer defence: Kyber secures communication between nodes and wallets to prevent interception, Dilithium verifies transactions and protects private keys from quantum attacks, and SPHINCS+ preserves the integrity of transaction records, turning each transaction into a unique, tamper-proof fingerprint.

Representative PQC Technologies

Source: Tiger Research, NIST

Technology	Security Layer	Underlying Principle	Strengths
CRYSTALS-Kyber (Key Exchange)	Communication encryption	Lattice-based KEM (Module-LWE)	Faster than RSA and ECDH, protects against MITM in quantum settings
CRYSTALS-Dilithium (Digital Signatures)	Transaction signature verification	Lattice-based signatures (Module-SIS + LWE)	Stronger quantum resistance than ECDSA, faster signature generation and verification
SPHINCS+ (Hash-based Signatures)	Record integrity	Hash-based tree structure	Long-term security, resistant to time-based attacks

Source: Tiger Research

Bitcoin is not a static system. In January 2026, the first "Bitcoin Quantum" testnets began experimenting with NIST-standardised PQC algorithms, such as ML-DSA (formerly Dilithium), demonstrating that these upgrades can be tested safely before network-wide implementation. These technologies help secure transaction processing, data transfer, and record storage, allowing bitcoin to remain resilient even in a quantum computing era. Past upgrades like SegWit and Taproot show that bitcoin can evolve safely while keeping the network fully operational.

Defence is not just technical, it is economic and social. A visible quantum attack would immediately threaten the network's value, incentivising miners, developers, exchanges, and major holders to coordinate a response. History shows that bitcoin forms consensus quickly around pragmatic solutions when systemic risks arise. Furthermore, quantum computing is developing gradually, giving bitcoin time to prepare, test, and deploy defences before the threat becomes real. In this case, protection, is about managing change carefully, not preventing it entirely.

Bitcoin's strength comes from both design and economics. Bitcoin has no central authority, headquarters, or off switch. Its ledger is maintained by thousands of independent nodes worldwide, removing single points of failure. Its fixed supply of 21mn coins protects against inflation, and its proof-of-work system, backed by massive computational power, makes large-scale attacks costly.

Global adoption further strengthens resilience. By 2024, roughly 500mn people held bitcoin or other cryptocurrencies. Institutional adoption has grown through ETFs, hedge funds, pension funds, and sovereign involvement. As bitcoin becomes embedded in the global financial system, the economic and political cost of attacking or destabilising it rises. Large stakeholders now have strong incentives to support its long-term stability rather than undermine it.

Some analysts, including Michael Saylor, have suggested that a transition to quantum resistant addresses could influence bitcoin's market dynamics. The argument is that if the network sets a "deadline" for migration, any coins that remain in old addresses because their owners lost the keys or are deceased would become permanently inaccessible. This would effectively remove millions of bitcoins from circulation, reducing the available supply and increasing scarcity. While the timing and market reaction remain uncertain, the potential impact of such an upgrade highlights the complex interplay between technological evolution and bitcoin's economic structure.

Conclusion

Quantum computing is not a threat limited to bitcoin, as many digital systems and internet communications rely on the same public-key cryptography that quantum computers could one day break. Notably, Nvidia CEO Jensen Huang has estimated that "very useful" quantum computers may still be 15 to 30 years away, giving the industry time to prepare. In the meantime, major technology companies are already taking steps to address the challenge. For example, Microsoft is integrating post-quantum cryptography (PQC) into core libraries and collaborating with international standards bodies to develop quantum-safe protocols for secure communication. These efforts show that both the broader tech ecosystem and the cryptocurrency world are beginning to anticipate and experiment with solutions, aiming to maintain security and trust across digital networks well before practical quantum computers arrive.

Welcome to Syzerland®

For further information

Banque Syz SA
Quai des Bergues 1
CH-1201 Geneva
T. +41 58 799 10 00
syzgroup.com

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Hugo Morel
Syz Research Lab Team
hugo.morel@syzgroup.com