Quantum Invasion on Blockchain

in-house seminar

Jeongho Jeon

2025-05-XX

DSRV (All That Node, Custody, Payments, Validator, WELLDONE Studio)

DISCLAIMER

I am not a cryptography expert.

Any undiscovered algorithm could invalidate this slide. P vs NP? Do we live in Cryptomania or Minicrypt?

Common Misunderstanding

Quantum computers do not excel at all tasks. Quantum computers excel at only a few problems: random circuit sampling, boson sampling simulation, finding ground states of quantum systems, and so on.

Some problems initially thought to show quantum advantage (or quantum supremacy) are later solved more efficiently with clever new classical algorithms. It's a cat-and-mouse game.

Unfortunately, the cryptography that current blockchains relies on are vulnerable to quantum computers. Shor algorithm (1994) and revised Oded Regev (2023) can find prime factors and discrete logarithms efficiently.

Quantum Computer news

In December 2024, Google unveiled the 105-qubit Willow chip, showing progress in reducing logical qubit error rates by increasing physical qubits using the surface code.

In January 2025, Nvidia CEO Jensen Huang stated during the CES keynote that it would take about 20 more years for quantum computers to become a reality.

Next week, Microsoft announced its enterprise quantum computing solution and revealed the Majorana 1 chip based on topological qubits in February.

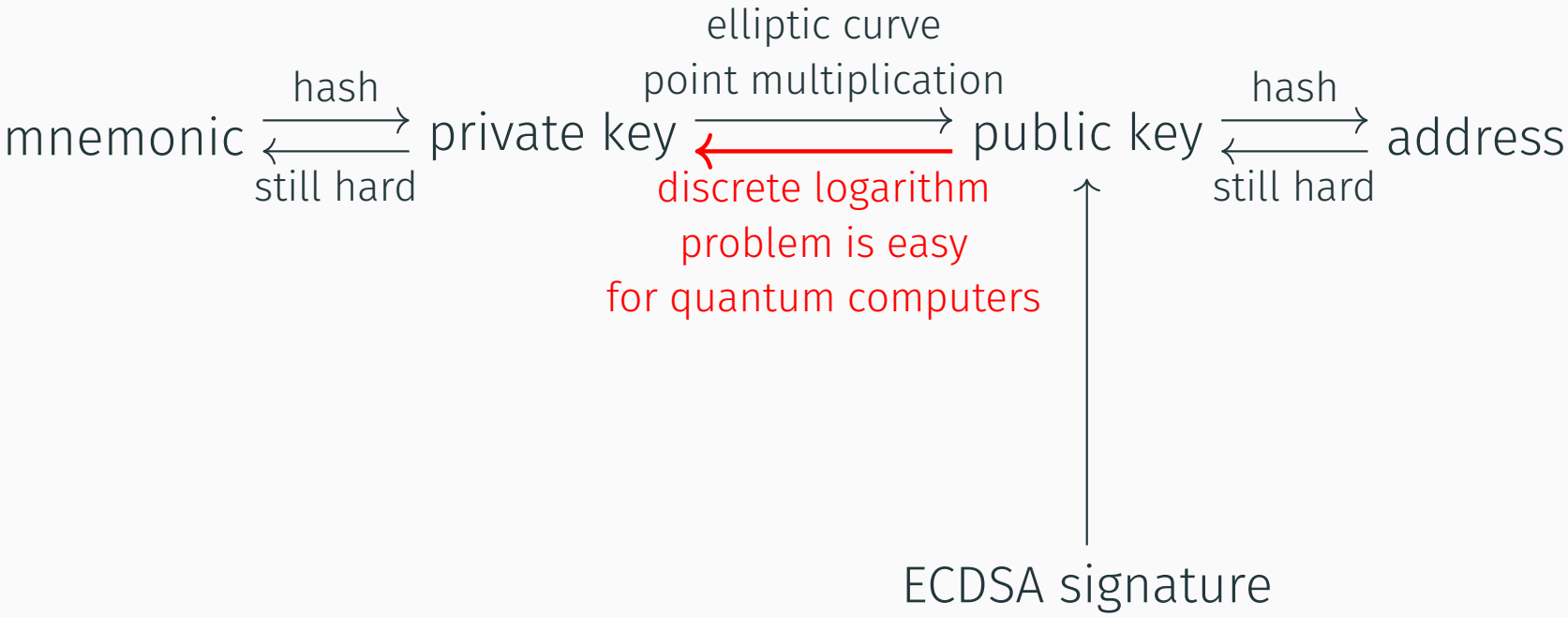
Each of these announcements led to significant volatility in quantum-related stocks and cryptocurrency prices.

Shor and Grover algorithms

Shor's algorithm can efficiently factor large integers and solve discrete logarithm problems ($O(a^n) \longrightarrow O(n^q)$). Introduced in 1994, it was the first example demonstrating the theoretical potential of quantum computers. Shor's algorithm can derive a private key from a public key.

Grover's algorithm accelerates unstructured search problems ($O(a^n) \longrightarrow O(a^{n/2})$), but isn't as disruptive as Shor's. It poses a theoretical threat to cryptographic hash functions, but simply doubling the hash length is enough to defend against such attacks.

Vulnerable point



Bitcoin price impact

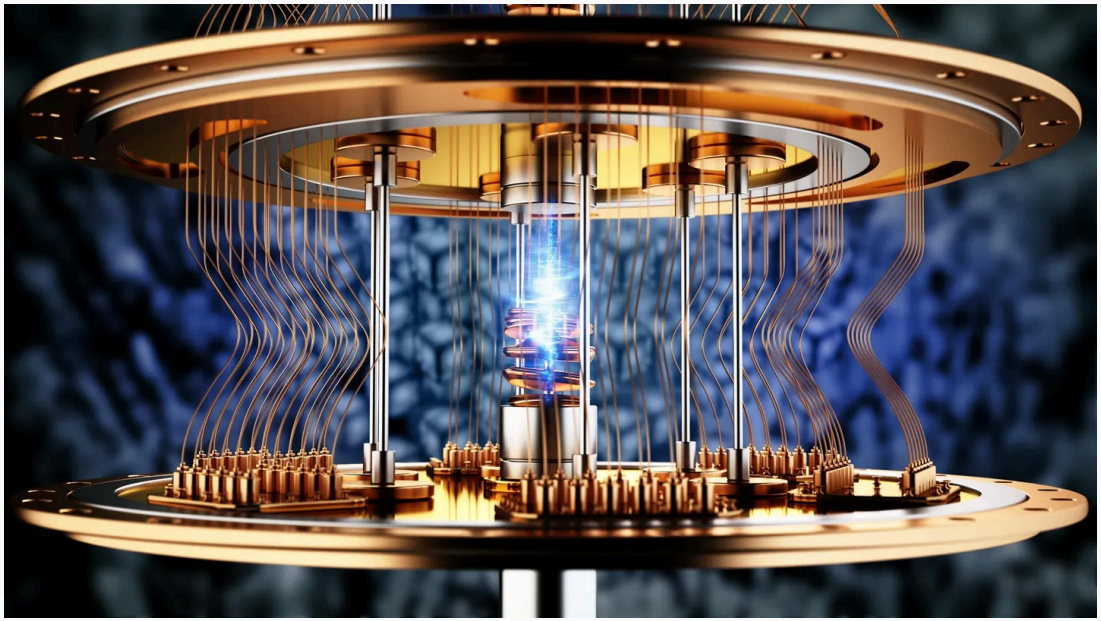
FORBES DIGITAL ASSETS

Google's Quantum Computing Leap: What It Means For Bitcoin's Security

By Ansel Lindner, Contributor. Ansel Lindner is an economist and Bitcoin & ... Follow Author

Dec 12, 2024, 04:51pm EST

Share Save Comment 0



Quantum computing breakthroughs and bitcoin security
GETTY

The recent announcement by Google CEO Sundar Pichai about their new quantum computing chip "Willow" has caused a few waves in the Bitcoin investment community and was like

Bitcoin case

In Bitcoin transactions, public keys can be exposed.

Early P2PK (pay to public key) transactions directly include the public key in the output part. Roughly 10% of all Bitcoin, including those believed to belong to Satoshi Nakamoto, fall into this category. Recent P2TR (Taproot) transactions also expose public keys.

P2PKH (pay to public key hash) transactions hide the public key until the coins are spent. At that point, all unspent tokens associated with the same address become vulnerable. The common Bitcoin practice of avoiding address can reduce public key exposure. Later P2WPKH (SegWit P2PKH), P2SH (pay to script hash) and P2WSH (SegWit P2SH) transactions may expose public keys when spent, too.

Public keys can also be revealed in mempool transactions before they are included in a block.

PQC (Post-Quantum Cryptography)

Cryptography relies on hard problems. For example, RSA is based on the assumption that factoring the product of two large primes is hard. For over 2,000 years, no efficient method for factoring large numbers has been discovered, so RSA has been trusted. But quantum computers break this assumption. We need problems that are hard even for quantum machines.

Algorithms based on lattice, code theory, hash, multivariate and supersingular elliptic curve isogeny are being proposed as quantum-resistant solutions. In 2022, after a 6-year competition, NIST selected 4 primary algorithms for standardization and continues to evaluate new candidates.

for encryption: (lattice-based) CRYSTALS-Kyber (ML-KEM), (new in 2025, code-based) HQC
for signature: (lattice-based) CRYSTALS-Dilithium (ML-DSA), Sphincs+ (SLH-DSA), (hash-based) FALCON (FN-DSA)

KpqC also finalized 4 PQC algorithms in 2025.

In 2022, an isogeny-based candidate, SIKE, relying on the SIDH assumption was broken and removed from the NIST selection.

Conclusion

Blockchain and PQC

Algorand, one of the few early adopters of PQC, has used the FALCON signature scheme since 2022. However, PQC tend to have larger key size and slower computation, which increase block size and verification time. This makes blockchains hesitant to adopt them.

Another concern is the relatively short history of these cryptographic assumptions. For comparison: factoring over 2,000 years, elliptic curves for 300 years (EC-DLP for 40 years), collision-resistant hashes for 50 years, and groups of unknown order for 20 years.

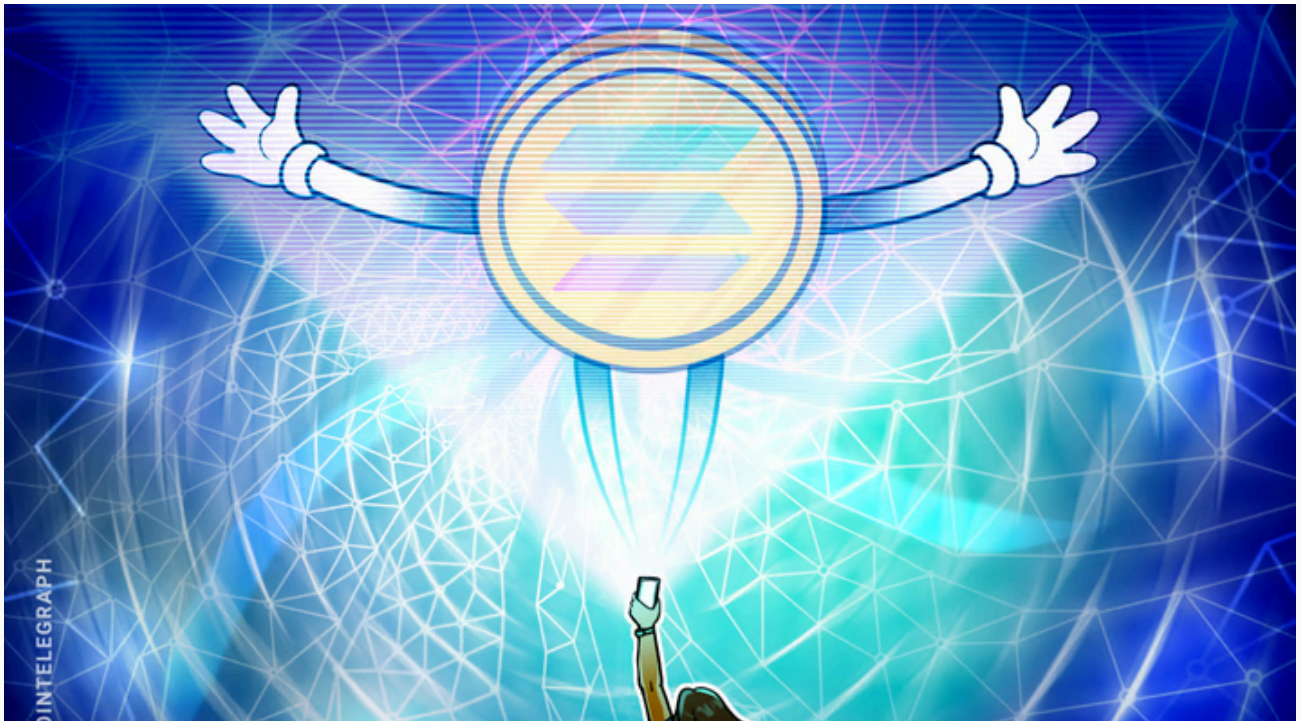
As a result, the idea of *cryptographic agility*, designing systems that can easily switch cryptographic primitives, is gaining traction.

BRAYDEN LINDREA

JAN 04, 2025

Solana is now quantum-resistant, Solana dev claims

The Solana Winternitz Vault is optional, meaning Solana users will need to choose to store their funds in the Winternitz vaults to be quantum-proof.



Solana news

A developer built a quantum-safe vault (token management smart contract) on Solana. Commands must be signed using hash-based signatures, secure against quantum computers. Solana native signature scheme is vulnerable to quantum computers, and it directly uses public keys as addresse without hashing. This smart contract approach adds quantum resistance without changing the protocol, and can apply to other blockchains, too.

A developer proposed a Bitcoin hard fork called the Quantum-Resistant Address Migration Protocol (QRAMP). The proposal requires users to move funds to Quantum-Resistant addresses secured by quantum-safe signatures. After a set deadline, transactions using legacy signatures would be rejected.

TECH

Share

Bitcoin Developer Proposes Hard Fork to Protect BTC From Quantum Computing Threats

The proposal outlines a plan to enforce a network-wide migration of BTC from legacy wallets to ones secured by post-quantum cryptography.

BY FRANCISCO RODRIGUES | EDITED BY AOYON ASHRAF

Apr 6, 2025, 2:00 a.m.

Ethereum case

Ethereum account abstraction (AA), including EIP-4337, EIP-7702 in upcoming Pectra hard fork and EIP-7701 in future, brings smart contract capabilities to regular accounts. One key benefit is support for new authentication methods such as 2FA and PQC.

Ethereum has other components that are also vulnerable to quantum attacks. See purple items in Vitalik roadmap.

- ECDSA signatures in transaction
- BLS signatures in consensus
- KZG commitments in blob
- Bandersnatch curve (tentative) in Verkle tree

Hash-Based Multi-Signatures for Post-Quantum Ethereum

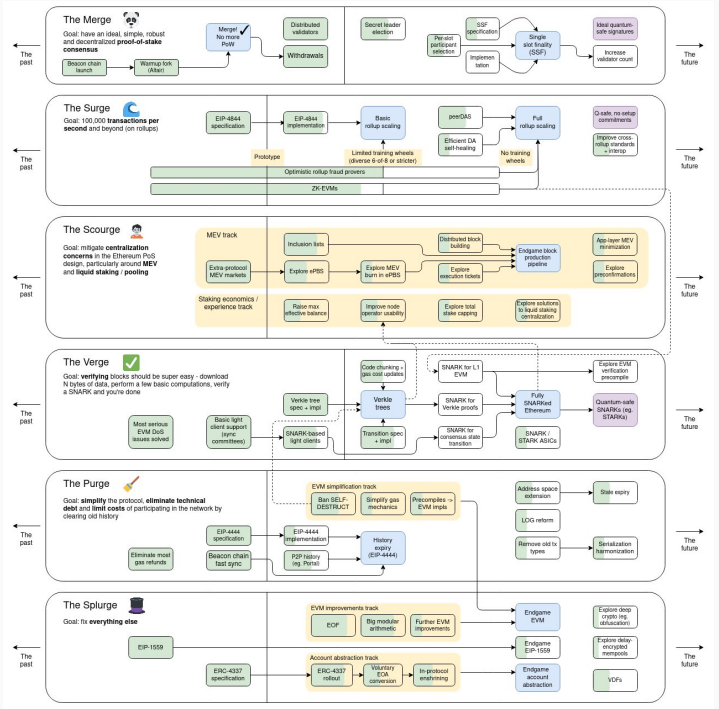
Justin Drake [1] Dmitry Khovratovich [1] Mikhail Kudinov*[2]
Benedikt Wagner [1]

[1] Ethereum Foundation
{justin.drake,dmitry.khovratovich,benedikt.wagner}@ethereum.org
[2] Eindhoven University of Technology
mishel.kudinov@gmail.com

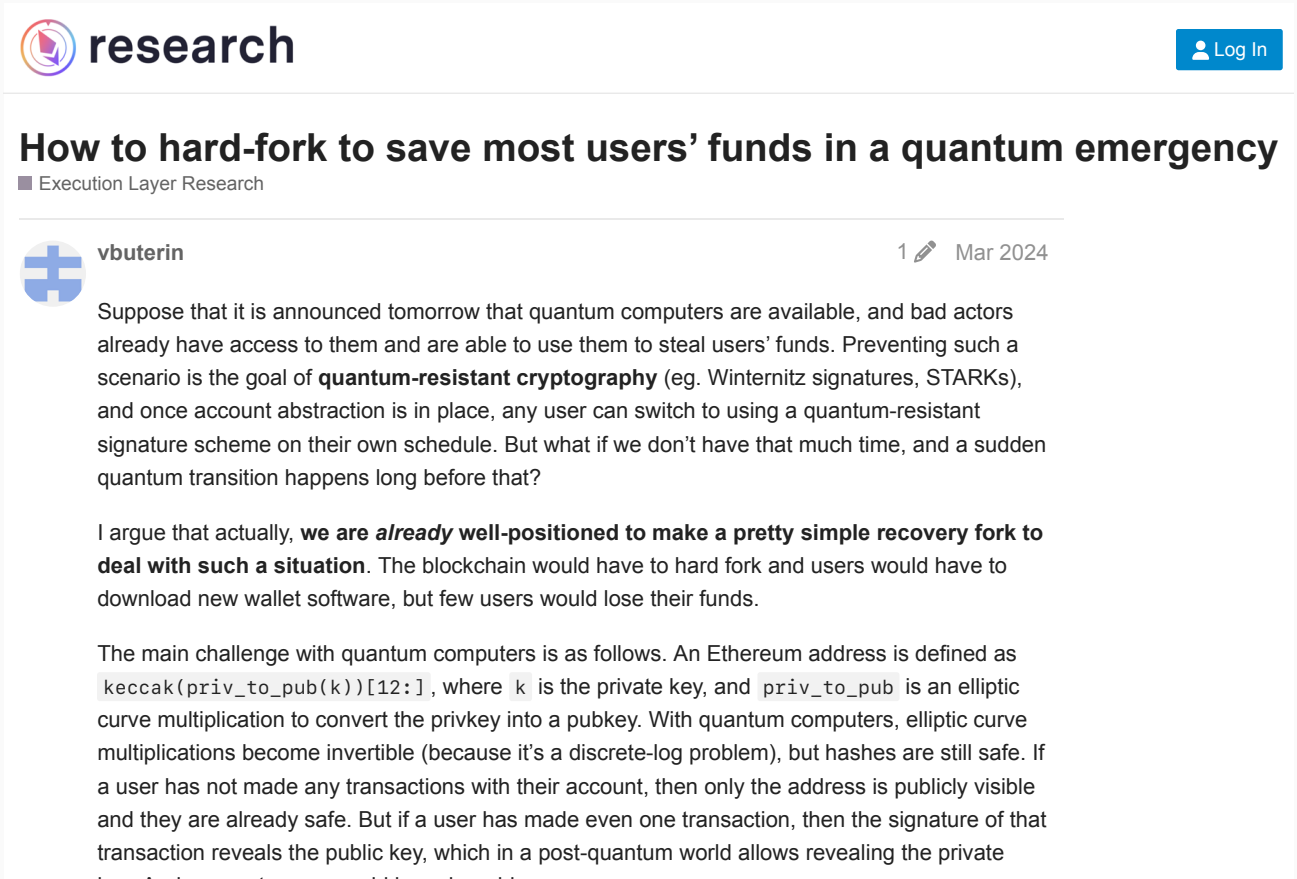
Abstract

With the threat posed by quantum computers on the horizon, systems like Ethereum must transition to cryptographic primitives resistant to quantum attacks. One of the most critical of these primitives is the non-interactive multi-signature scheme used in Ethereum's proof-of-stake consensus, currently implemented with BLS signatures. This primitive enables validators to independently sign blocks, with their signatures then publicly aggregated into a compact aggregate signature.

In this work, we introduce a family of hash-based signature schemes as post-quantum alternatives



Vitalik proposed an emergency hard fork in case quantum computers suddenly appear. The idea is to first roll back clearly compromised blocks and disable legacy transactions. Accounts can migrate to a quantum-proof state by submitting a new type of transaction that includes a quantum-resistant STARK zero-knowledge proof showing users know the mnemonic linked to their public key.



research

Log In

How to hard-fork to save most users' funds in a quantum emergency

Execution Layer Research

vbuterin 1 Mar 2024

Suppose that it is announced tomorrow that quantum computers are available, and bad actors already have access to them and are able to use them to steal users' funds. Preventing such a scenario is the goal of **quantum-resistant cryptography** (eg. Winternitz signatures, STARKs), and once account abstraction is in place, any user can switch to using a quantum-resistant signature scheme on their own schedule. But what if we don't have that much time, and a sudden quantum transition happens long before that?

I argue that actually, **we are *already* well-positioned to make a pretty simple recovery fork to deal with such a situation**. The blockchain would have to hard fork and users would have to download new wallet software, but few users would lose their funds.

The main challenge with quantum computers is as follows. An Ethereum address is defined as `keccak(priv_to_pub(k))[12:]`, where `k` is the private key, and `priv_to_pub` is an elliptic curve multiplication to convert the privkey into a pubkey. With quantum computers, elliptic curve multiplications become invertible (because it's a discrete-log problem), but hashes are still safe. If a user has not made any transactions with their account, then only the address is publicly visible and they are already safe. But if a user has made even one transaction, then the signature of that transaction reveals the public key, which in a post-quantum world allows revealing the private

Everyone's balance is publicly available, so it should always be possible to preserve this data, no matter what changes are made to BitCoin.

1NXYoJ5xU91Jp83XfVMHwwTUyZFK64BoAD

satoshi
Founder
Sr. Member

Activity: 364
Merit: 7750

Re: Dealing with SHA-256 Collisions
June 14, 2010, 08:39:50 PM
Merited by Raja_MBZ (3), ABCbits (2), vapourminer (1), bitcoinPsycho (1), vjudeu (1), livecoins (1)

#6

SHA-256 is very strong. It's not like the incremental step from MD5 to SHA1. It can last several decades unless there's some massive breakthrough attack.

If SHA-256 became completely broken, I think we could come to some agreement about what the honest block chain was before the trouble started, lock that in and continue from there with a new hash function.

If the hash breakdown came gradually, we could transition to a new hash in an orderly way. The software would be programmed to start using a new hash after a certain block number. Everyone would have to upgrade by that time. The software could save the new hash of all the old blocks to make sure a different block with the same old hash can't be used.

EricJ2190
Full Member

Activity: 134

Re: Dealing with SHA-256 Collisions
July 19, 2010, 12:44:17 AM

#7

Quote from: lachesis on June 14, 2010, 01:01:11 AM

A mathematician friend of mine pointed out that there are very few if any hash protocols that have

Hash collision asks whether it's possible to find or create two different inputs with the same hash output. If possible, it could rewrite past blocks linked by hash values. While there have been real-world attacks on hash functions due to unexpected weaknesses, but it's believed that quantum computers won't break collision resistance ($O(a^{n/2}) \longrightarrow O(a^{n/3})$ by Brassard–Høyer–Tapp algorithm).