

Forum: [Hack Forums](#)

Thread: [Quantum computers could bring lost Bitcoin back to life: Heres how](#)

Stanley - October 3, 2025, 4:05 pm

Quantum computers could bring lost Bitcoin back to life: Here's how

Quantum computing could enable the reverse engineering of private keys from publicly exposed ones, putting the security of Bitcoin holders at risk.

https://cointelegraph.com/explained/quantum-computers-could-bring-lost-bitcoin-back-to-life-heres-how?utm_source=rss_feed&utm_medium=rss&utm_campaign=rss_partner_inbound

INCREDIBLE - October 3, 2025, 6:06 pm

Of course. backward compatibility, like in video games.

Run Satoshi Nakamoto. They're coming!

Charlie Sheen - October 3, 2025, 8:52 pm

I really don't think they will let us have quantum computers. Governments will but we won't be allowed.

Vectura - October 3, 2025, 10:20 pm

That's both fascinating and scary. If quantum breaks Bitcoin's security, the whole crypto landscape could change overnight.

Fish - October 4, 2025, 3:44 am

Would be really interesting if this gets used. Who knows, maybe everyone will have quantum computers in the future?

Aeowulf - October 4, 2025, 9:24 am

(Oct 3, 2025 08:52 PM)Charlie Sheen Wrote: [\[CITE\]](#) I really don't think they will let us have quantum computers. Governments will but we won't be allowed.
100%

This would also just make everyday stuff used now... extremely obsolete. Everything is crackable. The next-gen stuff would be insane.

jcole - October 5, 2025, 12:45 pm

I'll take some forgotten wallets with a few Bitcoins.

Hackers - October 5, 2025, 1:31 pm

Quantum can complete certain computations in minutes, for what would take a modern super

computer millions of years.

In some cases, a regular computer would need more time than the age of the universe.
A quantum computer? Less than an hour.

AES-256 and other algos would still take a long time, but quantum would crack with a max of 2^{128} , and a classical computer has a max of 2^{256}

Both are astronomically hard to crack, but quantum already has a massive head start.

I believe I read that we would need 2 million qubits to reliably crack AES 256

With error correction methods, optimizations, and other new breakthroughs, maybe we can get this down

If you want to invest in companies, besides the top tech companies already:

IONQ

RGTI

QBTS

QUBT

B3A - October 6, 2025, 6:34 am

I dont thinkg quantum access will be public tbh

DAL-SHA - October 7, 2025, 1:01 am

Quantum computing is powerful but scary for Bitcoin security—could break keys and put many wallets at risk if not prepared soon.

though its very hard to build one !