

Forum:[Hack Forums](#)

Thread: [As Bitcoin Soars, Quantum Computing Raises New Questions About Its Security](#)

JoseMar - July 18, 2025, 7:13 am

As Bitcoin Soars, Quantum Computing
Raises New Questions About Its Security

Bitcoin is up. Like, really up. People are euphoric again. Discord channels full of laser-eyed memes, charts flying, everyone quoting PlanB like it's 2021.

But something feels weird this time. Maybe it's just me, or maybe it's the quiet conversation happening in the background, one that sounds more like math class than moon talk.

Quantum computing.

Not exactly clickbait, but stay with me. It's important.

You've probably heard this before, that quantum computers could break crypto someday. And yeah, it always felt like some 2049 problem, not a "should I be worried right now" problem.

But turns out... maybe we should. Or at least, we should be thinking about it more than we are.

The Core Problem (Literally, It's Math)

Bitcoin uses elliptic curve cryptography (ECC). It's how your wallet knows your coins are yours and not someone else's. Fancy math with hard-to-reverse problems.

Except that's the issue. Shor's algorithm, a quantum thing, can reverse them. Easily, eventually.

Think of it like this: everything keeping Bitcoin safe today is built on puzzles that are hard for classical computers... but not for quantum ones.

Once quantum computing hits that "relevant" level, the so-called Q-Day, anyone with one of those machines could, in theory, crack private keys.

That includes yours, mine, Satoshi's.

Capgemini's Wake-Up Slap

So there's this new report, Capgemini surveyed 1,000 big orgs in 13 countries.

70% are trying to prep for post-quantum cryptography.

But only 2% of cybersecurity budgets are actually going toward it.

It's like everyone knows the iceberg's out there but no one's moving the wheel.

Maybe because they don't know how. Or maybe because, like us, they're hoping it's just distant thunder.

Also: over 25% of all bitcoin has already revealed its public key. That makes it... pre-compromised, in a way. Not vulnerable today, but definitely not quantum-safe.

New entry for [7](#)contest?

? Big shoutout to [6](#) for making this even more exciting?

Hey guys, check this out.?

[DemonAsylum](#) [Braco22](#) [SUI-3183372](#) [SIM-1169085](#) [Walter](#) [HerrWinston](#) [Dystortion](#)

So Is Bitcoin Doomed?

I don't think so. Not exactly.
But it's going to have to change.

Some devs (like Jameson Lopp and crew) are already thinking ahead. They proposed a plan to "freeze" old coins that use legacy cryptography.

Yeah. Freeze. That's... dramatic.

But also, it might be the only way to protect dormant coins before quantum computers start sweeping them up like candy.

This proposal is bold, and honestly, kind of historic. Because Bitcoin usually doesn't change easily.

What's Actually Being Done?

Governments aren't just sitting around.

The U.S. NSA said it'll deprecate RSA and ECC by 2035.

NIST already picked new PQC algorithms, Kyber, Dilithium. (Cool names, surprisingly.)

Cloudflare, Apple, AWS, they're integrating them.

But blockchains? Not so much.

None of the top ten tokens are doing it yet.

Feels like crypto, the industry that's supposed to be ahead of the curve, is waiting till the last minute to study for the exam.

The Inevitable "So What?"

Maybe you're thinking: "Alright, but quantum computers aren't even here yet."

Fair. But there's this thing called harvest now, decrypt later.

Meaning attackers could be saving encrypted data now, betting that in 5–10 years, they can break it.

Including transactions, wallet details, and signatures from the blockchain you used today.

It's like someone copying your locked diary and planning to open it when they find the key... eventually.

This isn't a "sell all your BTC" moment.

But it is a moment to pause, maybe look at the fundamentals again.

The stuff that isn't on the charts, the math, the assumptions, the quiet clock ticking in the background.

We've always treated Bitcoin like it's invincible. But it was built in a world without CRQCs. That world's changing.

So yeah, Bitcoin's at a record high.

But some of the math behind it might be... not.

Just something to chew on before the next halving hype cycle hits.

Omniscient - July 18, 2025, 1:58 pm

https://github.com/jlopp/bips/blob/quantum_migration/bip-post-quantum-migration.mediawiki

This will get solved with a BIP years before it's a real threat. Just like the whole Bitcoin system upgraded from Native to Segwit wallets. And likely the wallets not upgraded (funds moved) will be open to the first groups to break encryption with Quantum Computers. Think of it as funding research. Cracking Satoshi's wallet, assuming it never moves, will be one giant multi-trillion dollar prize. Like lost pirate gold buried deep and found 500 years later. We are probably more than 20 years away from QC's having enough power to break BTC encryption.

Qubits required is in the millions when current tech is barely 1000.

AI Quote: You'd need 1,500–3,000 logical qubits (millions physical) to threaten Bitcoin's ECDSA security.

Current quantum computers are nowhere near this scale.

The crypto world is working on quantum-resistant alternatives well before this becomes reality.