

Forum:[Hack Forums](#)

Thread: [Monero Post-Quantum Research](#)

Omniscient - May 16, 2026, 2:44 pm

What happens if Monero updates to be Quantum proof before Bitcoin?

I remain very bullish on XMR. Use case (privacy) will never be topped by any other crypto.

Mr. Richie - May 17, 2026, 11:57 am

Monero needs more inventions, like the domain.eth-thingy.

Omniscient - May 17, 2026, 12:51 pm

(May 17, 2026 11:57 AM)Mr. Richie Wrote: [\[CITE\]](#) Monero needs more inventions, like the domain.eth-thingy.

Why? Do you ever use the ETH domain thingy? Bitcoin doesn't have it either.

Mr. Richie - May 17, 2026, 12:52 pm

(May 17, 2026 12:51 PM)Omniscient Wrote: [\[CITE\]](#) Why? Do you ever use the ETH domain thingy? Bitcoin doesn't have it either.

So the common man can use it.

Mastercarder - May 18, 2026, 7:47 am

If Monero becomes meaningfully post-quantum resistant before Bitcoin, it creates a very interesting narrative shift. Bitcoin still wins on institutional adoption, liquidity, and brand recognition, but Monero suddenly gains a huge edge in future-proof privacy + security. That combination is hard to ignore.

Most people still underestimate how important fungibility and privacy become once surveillance and chain analysis get more aggressive. XMR already dominates that niche. If it also becomes one of the first major quantum-resistant networks, that's a serious long-term value proposition.

Omniscient - May 18, 2026, 9:12 am

(May 18, 2026 07:47 AM)Mastercarder Wrote: [\[CITE\]](#) If Monero becomes meaningfully post-quantum resistant before Bitcoin, it creates a very interesting narrative shift. Bitcoin still wins on institutional adoption, liquidity, and brand recognition, but Monero suddenly gains a huge edge in future-proof privacy + security. That combination is hard to ignore.

Most people still underestimate how important fungibility and privacy become once surveillance and chain analysis get more aggressive. XMR already dominates that niche. If it also becomes one of the first major quantum-resistant networks, that's a serious long-term value proposition.

Just imagine how many people might swap their BTC for XMR just for security?

And btw, I'm actually very skeptical that quantum is a real threat to crypto anytime soon. But that's my personal opinion which many others don't share. There are a lot of panicked people who think Bitcoin is going to crumble soon and go to zero because of Satoshi's wallet and quantum. It's imho nonsense but the street perception can certainly move markets.

If XMR gets off their ass and make the chain quantum proof, huge win for the chain. I can see a

lot of people swapping and XMR immediately going past \$1k.

Mastercarder - May 18, 2026, 9:27 am

(May 18, 2026 09:12 AM)Omniscient Wrote: [\[CITE\]](#) Just imagine how many people might swap their BTC for XMR just for security?

And btw, I'm actually very skeptical that quantum is a real threat to crypto anytime soon. But that's my personal opinion which many others don't share. There are a lot of panicked people who think Bitcoin is going to crumble soon and go to zero because of Satoshi's wallet and quantum. It's imho nonsense but the street perception can certainly move markets.

If XMR gets off their ass and make the chain quantum proof, huge win for the chain. I can see a lot of people swapping and XMR immediately going past \$1k.

You make a fair point about the "street perception" side. Markets don't always move on reality, they move on narratives people believe could become reality. To be honest I still think people underestimate how hard it would be for Bitcoin to just get replaced though. BTC isn't only tech anymore, it's network effect, institutional trust, liquidity, ETFs, governments, infrastructure, etc. That moat is massive.

But for privacy-focused users? Different story entirely. If XMR ever became widely viewed as both truly private and more future-resistant than BTC, that could absolutely pull a serious amount of capital into the ecosystem. Especially during a fear cycle. The interesting part is that Monero doesn't even need Bitcoin to "fail" to benefit. It just needs enough people questioning surveillance, fungibility, and long-term privacy.

That's just what I think.

Omniscient - May 18, 2026, 9:34 am

(May 18, 2026 09:27 AM)Mastercarder Wrote: [\[CITE\]](#) You make a fair point about the "street perception" side. Markets don't always move on reality, they move on narratives people believe could become reality. To be honest I still think people underestimate how hard it would be for Bitcoin to just get replaced though. BTC isn't only tech anymore, it's network effect, institutional trust, liquidity, ETFs, governments, infrastructure, etc. That moat is massive.

But for privacy-focused users? Different story entirely. If XMR ever became widely viewed as both truly private and more future-resistant than BTC, that could absolutely pull a serious amount of capital into the ecosystem. Especially during a fear cycle. The interesting part is that Monero doesn't even need Bitcoin to "fail" to benefit. It just needs enough people questioning surveillance, fungibility, and long-term privacy.

That's just what I think.

I don't think XMR will replace but what people might do, swap BTC->XMR (Quantum Proof) -> BTC (Quantum Proof)

It might end up being a market-race to who is Quantum Proof first and almost for sure, it will be XMR. I'm a little surprised at myself for not thinking of this sooner and only recently coming across this info.

AI Quote: Monero (XMR) is not currently quantum-proof*, but the Monero community and Monero Research Lab have been actively researching post-quantum cryptography (PQC) for years. In fact, Monero is one of the few major cryptocurrencies openly discussing migration paths long before "Q-Day." ([ccs.getmonero.org][1])

The short version:

Today's Monero still relies heavily on elliptic curve cryptography (Ed25519 / Curve25519), which would theoretically be vulnerable to Shor's algorithm on a sufficiently powerful quantum computer. However, Monero's architecture and culture of regular hard forks make it more adaptable than Bitcoin for eventually transitioning to quantum-resistant cryptography. ([Reddit][2])

Here's the deeper breakdown.

What quantum computers threaten in Monero

Monero's privacy stack uses several cryptographic systems:

Stealth addresses Ring signatures / CLSAG
RingCT commitments Bulletproofs
ECC-based keys

Most of these rely on elliptic curve discrete logarithm assumptions, which a cryptographically relevant quantum computer could potentially break. ([Quantum Canary][3])

If a sufficiently advanced quantum computer existed:

Public/private keys could potentially be derived
Spend authorization could be forged Some transaction privacy guarantees could weaken
Old outputs whose public keys are exposed could become vulnerable

This is not unique to Monero. Bitcoin, Ethereum, and most major chains face the same core problem. ([Wikipedia][4])

Why Monero may adapt better than Bitcoin

This is where XMR gets interesting.

Monero already performs scheduled hard forks and major cryptographic upgrades more aggressively than Bitcoin. Examples:

RingCT
Bulletproofs CLSAG
Seraphis/Jamtis roadmap FCMP++ research

So culturally and technically, Monero users are already accustomed to protocol evolution. Bitcoin is far more conservative. ([MoneroSwapper][5])

That matters because migrating an entire blockchain to post-quantum cryptography is extremely disruptive.

Monero Research Lab (MRL)

[Monero Research Lab](
https://www.getmonero.org/resources/research-lab/?utm_source=chatgpt.com)

MRL has explored:

hash-based signatures lattice-based cryptography
post-quantum ring signatures hybrid schemes
post-quantum address systems migration strategies

A 2020 CCS proposal specifically researched “post-quantum Monero.” ([ccs.getmonero.org][1])

The challenge is brutal because Monero is not just securing balances:

it hides senders, hides receivers,
hides amounts, and prevents double-spending.

Doing *all of that privately with post-quantum math is far harder than simply replacing Bitcoin signatures.

Seraphis, Jamtis, and FCMP++

You’ll often hear these names in modern Monero discussions.

Seraphis

A next-generation transaction protocol redesign.

Jamtis

A newer addressing system tied to Seraphis.

FCMP++

A major privacy upgrade using Full Chain Membership Proofs.

These are not fully quantum-proof systems by themselves, but they modernize Monero’s architecture and make future PQ migration easier. ([Quantum Canary][3])

Recent discussions inside the Monero research community specifically mention:

PQ encryption for Jamtis
future hard forks including PQ mitigations hybrid cryptographic approaches

([GitHub][6])

One interesting Monero advantage

Monero’s privacy model may provide *some indirect protection compared to transparent chains.

Example:

Bitcoin exposes addresses and balances publicly forever.
Monero obscures ownership relationships and amounts.

So even if future quantum attacks become possible, an attacker has less immediately visible information to target. Some researchers and community members argue this gives Monero a softer failure mode than transparent ledgers. ([Reddit][7])

That said:

this is *not the same as being quantum-safe, and the underlying ECC assumptions are still vulnerable.

The biggest problem: migration

The hardest part is not inventing PQ cryptography.

The hardest part is:

migrating billions in existing outputs, preserving privacy,
avoiding deanonymization, avoiding chain splits,
keeping transaction sizes reasonable, and maintaining performance on consumer hardware.

Post-quantum schemes often have:

huge signatures, massive keys,
slower verification, or statefulness problems.

That is especially difficult for a privacy coin where transactions are already cryptographically heavy.
([arXiv][8])

Current realistic assessment

Right now:

No major cryptocurrency is truly “quantum-proof.” Monero is probably ahead of most projects in openly researching the issue.

But no production-ready fully PQ Monero exists yet.

Most cryptographers still believe practical attacks on ECC blockchains are likely many years away, though “harvest now, decrypt later” concerns are taken seriously. ([Reddit][2])

So the Monero approach today is basically:

1. acknowledge the threat,
2. actively research,
3. redesign architecture gradually,
4. prepare for eventual migration before quantum computers become practical.

[1]:

https://ccs.getmonero.org/proposals/research-post-quantum-monero.html?utm_source=chatgpt.com

"Research post-quantum strategies for Monero - CCS"

[2]:

https://www.reddit.com/r/Monero/comments/194h8cl/is_monero_quantum_resistant/?utm_source=chatgpt.com "Is monero quantum resistant?"

[3]:

https://www.quantumcanary.org/insights/can-quantum-computers-break-monero?utm_source=chatgpt.com "Can Quantum Computers Break Monero?"

[4]: https://en.wikipedia.org/wiki/Quantum_cryptography?utm_source=chatgpt.com "Quantum cryptography"

[5]: https://moneroswapper.com/blog/monero-after-quantum-computing?utm_source=chatgpt.com "Monero in a Post-Quantum World: How XMR Is Preparing ..."

[6]: https://github.com/monero-project/research-lab/issues/131?utm_source=chatgpt.com "Post-quantum security and ethical considerations over ..."

[7]:

https://www.reddit.com/r/Monero/comments/1n0ak76/is_there_any_serious_discussion_on_postquantum/?utm_source=chatgpt.com "Is there any serious discussion on post-quantum security ..."

[8]: https://arxiv.org/abs/2312.10430?utm_source=chatgpt.com "A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges"

Mewtwo - May 19, 2026, 2:41 am

I still don't understand what's driving ZEC above. I think XMR deserves that top 10.

If North Korea and Iran start using XMR instead of BTC/tether, it'll honestly be a really big push. It might sound like a horrible idea, but if no sanctions can defeat XMR, then it's really the ideal choice of anonymous and freedom. Nobody can control or govern what can be frozen or seized.

Even if the whole world bans XMR, there's really no stop to this at all lol.