

POST-QUANTUM RISK IN DIGITAL ASSETS

Why crypto can't simply migrate to post-quantum security

What actually has to happen on Bitcoin, Ethereum, Solana and TRON, why post-quantum signatures are larger, and why "it will hit banks too" misses the point.

AT A GLANCE

The protocol can build a safe destination. Only the holder can move there.

Every major blockchain secures ownership with elliptic-curve signatures that a large enough quantum computer can break. Chains can add post-quantum (PQ) signatures, but nobody can move coins on a holder's behalf, so migration means millions of independent people acting in time.

<500k

Physical qubits Google now estimates are needed to break Bitcoin and Ethereum's curve, down about 20x

PostQuantum

~9 min

Estimated key-specific attack time once a public key is revealed, shorter than one Bitcoin block

PostQuantum

6.9 M BTC

Up to 6.9M BTC already sit in addresses with exposed public keys, including about 1.1M attributed to Satoshi

VanEck

0 of 30

Top networks by TVL that had completed a mainnet PQ migration in Quantum's March 2026 audit

Quantum research

Six things to remember

01

Migration is a people problem

Upgrading the protocol is the easy part. Every holder has to move their own funds, and lost or dormant coins can never move at all.

02

A wallet is only as safe as its chain

Consensus, bridges, issuer admin keys and proofs all use classical keys. A PQ wallet protects one key, not the system around it.

03

PQ wallets protect keys, not value

When unmigrated coins are stolen and sold, the price falls for everyone, including holders who migrated perfectly.

04

Decentralization slows migration

A bank can migrate by decree. Bitcoin can only migrate by persuasion, one key holder at a time.

05

Banks are not the same case

Banks have identity, law, reversibility and regulators behind ownership. In crypto, the key is the ownership, and it sits on a public ledger forever.

06

The target keeps getting cheaper

Attack estimates keep falling while migration takes years, so the time to start is well before any machine exists.



01 / FORKS

A fork changes the rules, not who holds the coins

A fork can teach a chain to accept post-quantum signatures, but it can't sign for anyone. Whichever route a chain takes, it ends the same way, with each holder moving their own coins.

ROUTE 1

Soft fork

WHAT IT IS

Stricter rules that old nodes still accept, so the chain doesn't split (CoinGecko)

PQ EXAMPLE

Bitcoin's BIP-360 adds an output type without Taproot's exposed key path, as a first step toward PQ signatures (StarkWare)

CATCH

Needs about 90% of miners to signal. Taproot took nearly four years from idea in 2018 to activation in 2021 (Galaxy)

ROUTE 2

Hard fork

WHAT IT IS

New rules that old nodes reject, so everyone must upgrade or the chain splits (Fidelity Digital Assets)

PQ EXAMPLE

Ethereum's scheduled upgrades, or an emergency fork that disables old accounts and lets users recover with a proof (Ethereum Research)

CATCH

Contested forks split chains, as with Ethereum Classic in 2016 and Bitcoin Cash in 2017. On Bitcoin it is close to unthinkable

ROUTE 3

No fork: StarkWare's QSB

WHAT IT IS

A hash-based lock built from Bitcoin's existing script rules, first mined on mainnet on 26 August 2026 (StarkWare)

PQ EXAMPLE

A holder moves coins into a QSB output that a quantum computer can't open

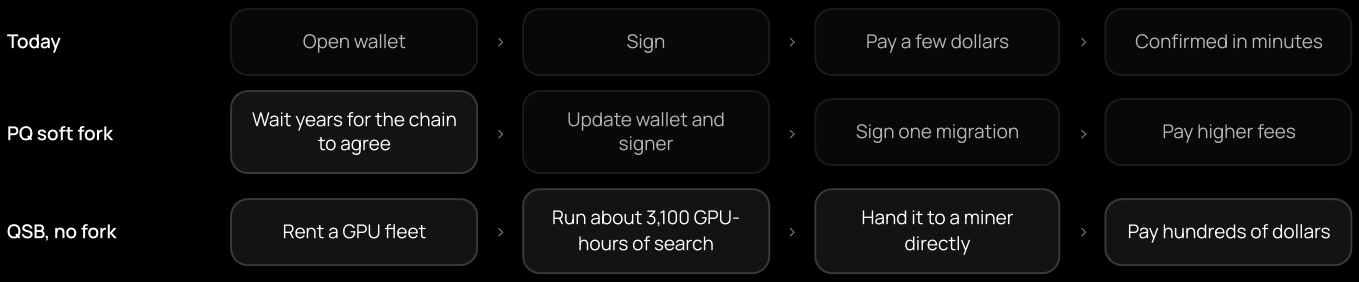
CATCH

StarkWare calls it a last resort and still sees a soft fork as the long-term fix (StarkWare)

Bitcoin realistically only has the slowest route.

Bitcoin upgrades by soft fork and has historically rejected hard fork attempts, because they split the community and the market into two chains (Fidelity). The route with the fewest risks is also the one that takes the longest to agree on.

What a holder has to do



Lighter boxes are steps a normal user can do today. Darker boxes need coordination, specialist tooling or capital.

What each route means for the user

	TODAY	AFTER A PQ SOFT FORK	QSB, NO FORK
Effort	Tap send	Update the wallet, then send one migration transaction	Run a GPU search before sending. The first one took about 3,100 GPU-hours on 100 GPUs (StarkWare)
Cost	A few dollars in fees	Higher fees, because PQ signatures are 10-110x larger	About $75-200 in compute on top of fees (QRL), and about $320 for the first one
Broadcast	Any node	Any node	Non-standard, so it must go straight to a miner such as MARA Slipstream (Cointelegraph)
Compatibility	All wallets	Wallets and hardware signers that adopt it	Legacy scripts only, so no SegWit, Taproot or Lightning (QRL)
Exposed keys	Not protected	Protected only once moved	Not protected if the key was already public (StarkWare)

Every route still ends with the holder signing a transaction. A fork decides what is possible, but only holders decide what actually moves.

QSB proves Bitcoin can protect individual coins without consensus, but at hundreds of dollars and a specialist workflow per transaction it is a lifeboat for a few holders, not a migration for millions.

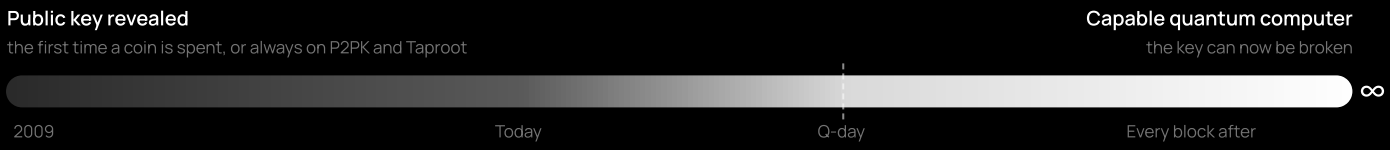
02 / THE THREAT

Breaking crypto keeps getting cheaper

No machine of this size exists yet. The point is that migration takes years while the estimated cost of an attack keeps falling.

- In March 2026, Google Quantum AI, with the Ethereum Foundation and Stanford, put the cost of breaking the 256-bit curve at about 1,200-1,450 logical qubits and fewer than 500,000 physical qubits, roughly 20x below earlier estimates (PostQuantum).
- The ECDSA.fail paper, co-authored by Quantum's Chief Researcher and a senior engineer, documents a community effort that cut a key secp256k1 attack benchmark by more than half (Quantum on X, arXiv).
- As Professor Jens Eisert explained on Quantum's podcast, the noisy qubits needed to break RSA have fallen from 20 million in 2019 to under one million today (Quantum on X).
- In a 2024 survey, 17 of 32 leading quantum researchers put the chance of a cryptographically relevant machine within 10 years above 5% (Global Risk Institute).

A blockchain never forgets



A ledger keeps every record for as long as validators keep validating it, and every node holds a full copy. A public key published in 2010 is still readable today and will still be readable on the day a quantum computer can break it. Nothing expires and nothing can be deleted, so the only defence is to move the coins before that day. Realistic estimates of 11-19 years for development, consensus, deployment and user migration already exceed many threat timelines (Campbell, JBBA).

03 / ETHEREUM

Why ETH can't simply migrate

Ethereum has the most credible PQ program of any major chain, which makes it the clearest example of how hard this is even in the best case.

Four layers need new cryptography

Validators	Data	Accounts	Proofs
BLS signatures that finalize every block	KZG commitments behind data availability	ECDSA signatures on every ordinary wallet	ZK proof systems used by rollups

Source: Mitrade

> **Target: December 2029 for the protocol, and more years after that for the ecosystem to actually move.**
>
> That means about five hard forks at an average of 7.2 months each (Ethereum Foundation). The EF's own PQ team expects full execution-layer migration to take additional years beyond 2029 (pq.ethereum.org).

Why it stays hard

- An ordinary account is bound to its ECDSA key, because the address is derived from it. Native account abstraction (EIP-8141) lets users switch to PQ keys on their own schedule (ethereum.org, CoinDesk), but because it is opt-in, some users will never do it.
- Deloitte estimated that about 65% of all ETH sits in quantum-exposed accounts (Deloitte).
- Vitalik Buterin's emergency plan would roll back the chain, disable classic accounts and let users recover with a STARK proof of their seed phrase. It does not establish a path for keys without that derivation (Ethereum Research), and a rollback would be a major social and legal event.
- Three migrations overlap: ECDSA to PQ, the EVM toward RISC-V, and the state tree to a new structure and hash. Running them in parallel adds risk, and running them one after another adds years.



04 / HOLDERS

Every holder has to act

Usually the move is to a new PQ address on the same chain, not to a separate "PQ chain". A bridge to another chain is only needed if the original doesn't upgrade in time or splits. Either way, only the key holder can make the move.

76-142 days

To migrate every Bitcoin UTXO if migration used all block space

305-568 days

If migration used a more realistic 25% of block space

5-15 yrs

Full timeline for research, BIPs, deployment and migration

Chaincode estimates via Jameson Lopp. A more optimistic view says 90% of BTC value could move in about 4 days, because value sits in relatively few UTXOs (Presidio Bitcoin). The bottleneck is people, not blocks.

What makes this hard

- On Bitcoin, BIP-360 (P2MR) is only a first step. It does not choose a PQ signature, which needs a follow-on soft fork (Galaxy).
- Lost keys, deceased owners and dormant early coins can never move. One analysis puts about 2.3M BTC as irreducibly at risk (arXiv).
- That forces a choice with no good answer. BIP-361 would freeze unmigrated coins after a sunset period, so the community is choosing between frozen coins and stolen coins (CryptoSlate).
- Hardware wallets may need new firmware or new devices, and institutional and air-gapped signing workflows all need rebuilding.
- The migration window is also the attack window. Millions of keys get revealed in a short period, under fee pressure.

05 / WALLETS

A wallet can't be safer than its chain

An asset is only as quantum-safe as the weakest key that can move it, mint it, freeze it or finalize it. A vault door doesn't help if the walls are glass.

Your PQ wallet	Protects your own key	PQ
Consensus	Ethereum validators sign with BLS, and Solana validators and votes use Ed25519 (arXiv)	CLASSICAL
Asset issuer	Admin keys can mint, freeze or upgrade the token, like TRON's USDT multisig (Cryptopolitan)	CLASSICAL
Bridges and apps	Bridges, oracles, sequencers, multisigs and DeFi contracts	CLASSICAL
Data and proofs	KZG commitments and pairing-based ZK proofs such as Groth16	CLASSICAL
Fees and infrastructure	Fee payers and network signatures stay on elliptic curves even with Solana's Winternitz vaults (arXiv)	CLASSICAL

MPC and threshold signing don't fix this either. The combined signature is still a single elliptic-curve key on-chain.

PQ wallets protect keys, not value.

Quantum's internal model estimates $147-278B in stealable orphaned coins across BTC, ETH, SOL, BNB and XRP, meaning lost or abandoned holdings whose keys are already exposed (March 2026 prices). Across scenarios, theft and resale could erase from about $150-250B to $1.0-1.4T of market value. These are scenario estimates, not forecasts, but the mechanism holds: on a shared ledger, your security depends on everyone else's migration.

06 / CONCENTRATED RISK

Stablecoins and bridges are the biggest targets

Most value doesn't sit in individual wallets. It sits behind a small number of privileged keys.

Stablecoin admin keys

Every major stablecoin relies on admin keys that can mint, burn, freeze, pause and upgrade. Deriving one of them allows unlimited minting and breaks the peg, and the attack is silent because the derived key is valid (Project Eleven).

The power is real

Tether froze about $3.29B across 7,268 addresses between 2023 and 2025 (AMLBot), which shows how much a single compromised key would control.

Bridges use small signer sets

The largest bridges include custodial WBTC on a BitGo multisig and Wormhole, where 13 of 19 guardians approve any message (DefiLlama). An attacker would only need to derive 13 keys, and every one is exposed on-chain with each attestation.

Already the weakest link

Bridges caused 47% of all DeFi exploit losses as of May 2024, without any quantum capability (ACM).

Stablecoin issuers and custodians will probably move first.

They decide centrally, they are regulated like financial institutions, and losing one key could destroy the whole asset.

07 / CHAIN BY CHAIN

Where each chain stands, October 2026

Chains that are more centralized can ship faster. On every chain, though, users still have to act, old keys stay exposed, and issuer and infrastructure keys need separate work.

CHAIN	KEY EXPOSURE	PQ STATUS
Bitcoin DRAFT ONLY	Older address types hide the key until its first spend, but Taproot exposes it directly. 6.5-6.9M BTC are already exposed (VanEck)	BIP-360 and BIP-361 are still drafts, and nothing PQ is live (VanEck). Governance is the binding constraint (Cointelegraph)
Ethereum ROADMAP	An account's key becomes public after its first transaction	December 2029 for all L1 layers, with execution-layer migration taking longer (pq.ethereum.org)
Solana CONDITIONAL	Worst case: the address is the public key, so it is exposed from creation (Hardy Index)	Falcon was chosen, but the plan is conditional with no dates (Solana). The opt-in Winternitz vault had fewer than 300 accounts (Hardy Index)
TRON TESTNET	Same as Ethereum	FN-DSA-512 has been on the Nile testnet since July 2026, with no mainnet date (Ground News). Gaps remain in seed recovery and Ledger support (Bitcoin Foundation)

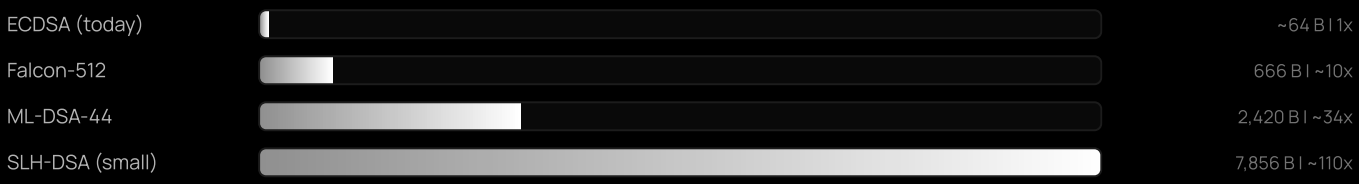
Shipping fast brings its own risk, which is why Quantum has publicly urged TRON to put its upgrade through rigorous internal testing and independent external review before mainnet (AMBCrypto). Across the market, the closest any network got in Quantum's March audit was Algorand, with Falcon state proofs live since 2022 (Algorand), but its consensus is not yet PQ.

08 / SIZE

Why PQ cryptography is larger

Elliptic curves are unusually compact, because there is no known efficient classical attack on them. A 32-byte key and a 64-byte signature give about 128-bit security. PQ schemes rely on different hard problems, and those need far more data.

Signature size, drawn to scale



Public keys grow too, from 33 B for ECDSA to 897 B for Falcon-512 and 1,312 B for ML-DSA-44. Faster SLH-DSA variants reach 49,856 B. Sources: CEUR-WS, IACR ePrint

Lattices

ML-DSA and Falcon store keys and signatures as large arrays of polynomial coefficients.

Hashes

SLH-DSA, XMSS and Winternitz build each signature from many hash values, and some keys can only be used once.

No aggregation

PQ signatures can't be combined the way BLS signatures can, so Ethereum needs a separate zkVM to compress them (pq.ethereum.org).

What it does to a chain

- On Bitcoin, a block that holds 2,500-3,000 standard transactions would fit only 500-700 PQ transactions, a 4-5x drop in throughput with fees to match (PostQuantum).
- On Ethereum, leanXMSS replaces 96-byte BLS signatures with signatures of nearly 3,000 bytes (Mitrade).
- Fast chains like Solana, Sui and Aptos depend on batch signature verification, and no efficient PQ version of it exists yet.
- Every wallet, hardware signer, HSM, custody system, bridge and dApp that checks signatures has to change.
- The newer schemes carry their own risk. Bitcoin's SHRINCS proposal still lists its security proof as "TODO" (Cointelegraph), and Falcon is susceptible to side-channel attacks (JBBA).

09 / DECENTRALIZATION

The more decentralized the chain, the harder the migration

> **A bank can migrate by decree. Bitcoin can only migrate by persuasion, one key holder at a time.**

MIGRATES BY DECREE		MIGRATES BY PERSUASION	
Banks and issuers	**TRON**	**Ethereum, Solana**	**Bitcoin**
Central decision, mandated deadlines, can rotate keys	Small validator set, fast to ship, users still must act	Coordinated roadmaps, opt-in for users	Most conservative, no authority over dormant coins

Why decentralization adds friction

No one can act for you

No one can rotate keys or move funds on a holder's behalf.

Consensus is voluntary

Every change needs social agreement, and the most conservative chains change most slowly.

Dormant coins have no owner

No one can be reached and no one has the authority to decide what happens to them.

The past can't be hidden

An immutable ledger can't conceal public keys that are already exposed.

Decentralization isn't the only factor. Building in flexibility, like Ethereum's account abstraction, cuts friction considerably, but it still can't force anyone to act.



10 / THE BANKS ARGUMENT

"If quantum breaks crypto, it breaks banks too"

This is the most common pushback, and it doesn't hold. "Everything breaks" is a false binary, because PQ cryptography is standardized and already being deployed. The systems that upgrade will be safe and the ones that don't will be broken. Banks are being made to upgrade, while blockchains have to persuade millions of holders to do it.

	BANKS	CRYPTO
What protects ownership	Identity, KYC, contracts, law, insurance and the central bank. Cryptography protects only the channels	Only cryptography. Whoever holds the key owns the asset
Where the keys live	Private, in HSMs, rotated behind closed doors with no public record	Public keys published on an immutable ledger, permanently
Main algorithm	A mix that leans on RSA	Almost all elliptic-curve, with keys about an order of magnitude smaller than RSA's, so a smaller machine breaks them first (Forbes)
After a theft	Recall, freeze, chargeback, insurance	Final. The coin is gone once the attacker's transaction confirms
Who drives migration	Regulators with deadlines, plus a CISO at every bank	Volunteers. Nobody can mandate it
Appeal to attackers	Data and channel breaches that can be contained	Bearer, pseudonymous, liquid and irreversible, which makes it the most monetizable first target

The details behind it

- Same family of math, used differently. Banks do use ECDSA on P-256 and RSA in TLS, SWIFT, cards and apps, and Shor's algorithm breaks all of it (PostQuantum). The difference is architecture, not algorithm. Solana uses Ed25519 and Taproot uses Schnorr, so the precise term is "elliptic-curve signatures".
- Mandates are already set. NIST deprecates quantum-vulnerable algorithms at 112-bit security after 2030 and disallows all of them after 2035 (NIST IR 8547). The EU wants critical sectors, including finance, upgraded by the end of 2030 (PostQuantum), MAS is targeting the end of the decade (PostQuantum), and the BIS has a sector-wide roadmap (BIS).
- The first actor with a capable machine is unlikely to announce it. They are more likely to quietly drain cold storage, treasuries and dormant whales, with no human to social-engineer, just math against math.
- Where the argument has a point: banks do face "harvest now, decrypt later" risk to confidential data (PwC), and an uncoordinated transition could leave weak links (BIS). But a breach of data can be contained and compensated. In crypto, the same break is an irreversible transfer of ownership.



11 / COMMON OBJECTIONS

What people get wrong

MYTH

"My coins are safe because I've never spent from the address."

REALITY

This only works where the address is a hash of the key. Taproot and every Solana account expose it from day one (arXiv). The moment you spend, the key is revealed, and with an attack time of about 9 minutes it can be raced in the mempool (PostQuantum). Address reuse, shared xpubs and signed messages leak keys too, a sunset like BIP-361 would freeze the coins anyway (BIP-361), and if a third of supply is stolen and dumped, your hidden coins lose value with everyone else's.

MYTH

"Just add PQ wallets to existing chains."

REALITY

Wallets cover custody only. Consensus, bridges, issuer keys, data availability and ZK proofs stay exploitable, and institutions won't accept "we patched the wallet" as a complete answer.

MYTH

"It's just a minor upgrade."

REALITY

Signatures get 10-110x bigger, which changes block limits, fees, hardware and every app that verifies signatures. On Ethereum it overlaps with two other major migrations.

MYTH

"Nobody is attacking anything yet."

REALITY

The EU says harvest-now-decrypt-later attacks are "likely occurring already now" (EUR-Lex). A blockchain is the ultimate archive to harvest, because every exposed key is already public.

MYTH

"Upgrade once and you're done."

REALITY

PQ schemes are young, so chains may have to switch algorithms again. The ability to swap algorithms matters more than any single algorithm.

MYTH

"Markets will react when coins are actually stolen."

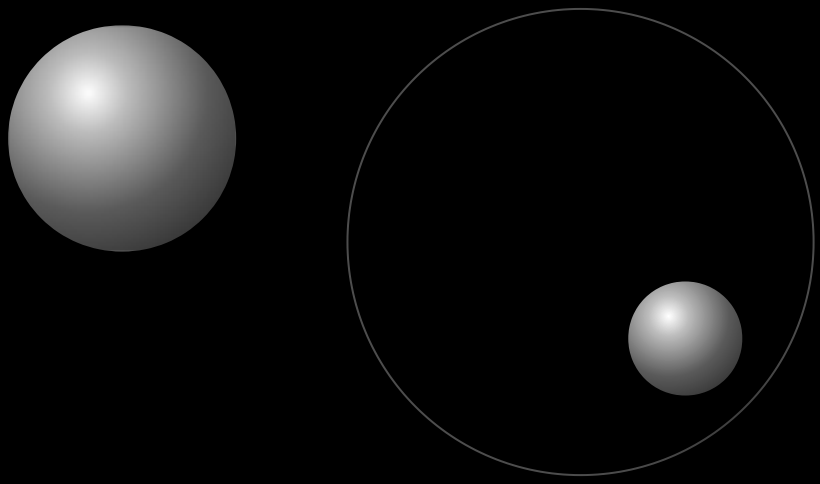
REALITY

Credible demonstrations, fights over freezing coins and failed upgrades can reprice assets long before any theft.

BOTTOM LINE

Quantum risk in crypto isn't a cryptography problem with a software patch. It's a coordination problem across protocols, issuers, custodians and millions of holders, and if it fails, the losses are irreversible.

Banks can be made to migrate and can make customers whole. Chains can only offer a safe path and hope their holders take it in time. The chains, issuers and custodians that build verifiable PQ migration paths now will be best placed when the market starts to price this risk.



ABOUT QUANTUM FOUNDATION

Quantum Foundation builds post-quantum security infrastructure: the SDKs and building blocks that exchanges, custodians, wallets and L1 teams need to move to post-quantum security, including post-quantum MPC custody with co-signers, EVM post-quantum verification, open-source ML-DSA, ML-KEM and SLH-DSA packages, and a Rust developer toolkit.
quantum.phd · @QuantumFDN · info@multivmlabs.com

QUANTUM

Quantum Foundation. Post-Quantum Security Infrastructure. Prepared by Quantum Foundation (MultiVM Labs) from its Knowledge Hub research and current public sources. Figures are as of October 2026 unless noted. Quantum's internal estimates are scenario models, not forecasts.