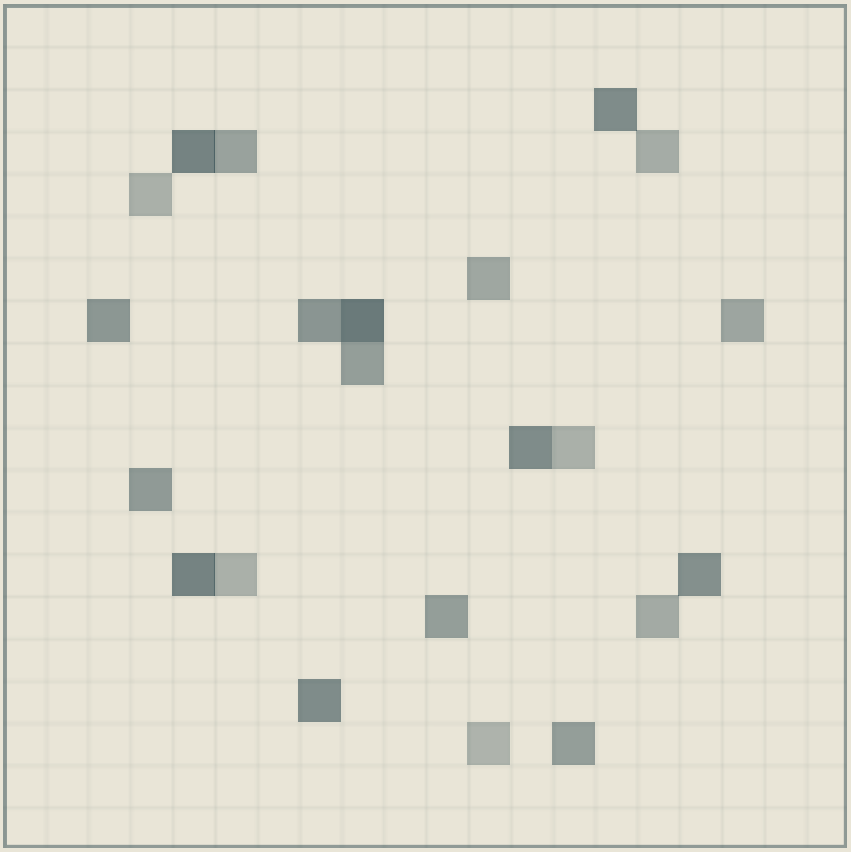
POST-QUANTUM CUSTODY FOR TOKENS ON SOLANA

STARK MACHINA



Stark Sentinel
starkmachina.com
x.com/stark_machina

Abstract

A token on a public blockchain is guarded by a digital signature scheme that a sufficiently large quantum computer will break. The elliptic-curve keys securing balances on Solana, Bitcoin, and Ethereum were never designed to survive Shor's algorithm, and the attack has already begun: signed and encrypted data recorded today can be broken the day the hardware arrives, a strategy known as harvest now, decrypt later. STARK MACHINA is an opt-in custody overlay that moves a holder's spend authority off exposed elliptic-curve keys and onto NIST-standardised post-quantum signatures before that day, Q-Day, comes. A holder enrolls with a single signature, deposits into a Token-2022 Quantum Vault, and delegates transfer authority, for that amount only, to an autonomous agent called the Sentinel, bound by a fixed directive it cannot deviate from. The Sentinel migrates the vault onto lattice-based (ML-DSA-44) and then hash-based (SLH-DSA) signatures, rotates keys forward-securely, and publishes a falsifiable custody score with every action it takes. Staked supply earns SOL yield, funding the security budget that must last the years to Q-Day. What one guarded token proves, an open network of tokens can inherit.

1. Introduction

In 1993 Eric Hughes wrote that privacy is necessary for an open society in the electronic age, and that cypherpunks would defend it not by asking for it, but by writing code. Cryptography has always been defensive infrastructure. It is the one tool that lets an individual hold a position against a far larger adversary and win, because the cost of defense and the cost of attack are separated by mathematics rather than by force. The cypherpunks understood that the guarantee was never permanent. It held only for as long as the underlying problem stayed hard.

Public-key cryptography rests on problems believed to be intractable for classical computers: integer factorisation and the discrete logarithm. Every wallet on every major chain inherits that assumption. Bitcoin, Ethereum, and Solana authenticate ownership with elliptic-curve signatures whose security reduces to the discrete logarithm being hard. In 1994 Peter Shor showed that a quantum computer could solve both problems in polynomial time. The assumption does not weaken gradually. It fails on a threshold, and everything built on it fails at once.

For thirty years this was a distant concern. It is no longer distant. Standards bodies have set migration deadlines, national laboratories publish credible hardware timelines, and the defensive algorithms have been finalised and standardised. The missing piece is not the cryptography. It is deployment, at the layer where ordinary holders actually keep their assets, before the window closes. STARK MACHINA is that deployment.

2. The Quantum Threat

Shor's algorithm breaks the signature schemes that secure digital assets: RSA, ECDSA on Bitcoin and Ethereum, and Ed25519 on Solana. Once a cryptographically relevant quantum computer exists, any public key that has been revealed on-chain can be inverted to recover its private key, and the holder's assets can be spent by whoever runs the machine first.

The danger does not begin on Q-Day. It has already begun. *Harvest now, decrypt later*, known in enterprise security as Y2Q, the Year to Quantum, describes adversaries recording signed and encrypted data today in order to break it retroactively once the hardware is available. A blockchain is the ideal target: it is a permanent, public, complete archive of every signature ever produced. Nothing needs to be intercepted. It is already published, and it is waiting.

The margins are thinner than they appear. Published research indicates that a sufficiently powerful quantum computer could derive a Bitcoin private key from an exposed public key in roughly nine minutes, against a block time of ten. The safety interval is a single minute of arithmetic. Ethereum faces the same exposure across more than one hundred million active wallets and is already designing a migration path. These are not fringe positions. They are the stated planning assumptions of the ecosystems themselves.

Credible estimates for when a relevant machine arrives cluster within a decade:

- **2029**, Google research trajectory.
- **2030**, the migration deadline set by NIST and the NSA for federal systems.
- **2033**, industry hardware roadmaps.
- **2035**, the Global Risk Institute's fifty-percent-probability estimate.

The defensive standards are already finished. In 2024 NIST finalised the first post-quantum signature standards: FIPS 204 (ML-DSA, the lattice-based CRYSTALS-Dilithium family) and FIPS 205 (SLH-DSA, the hash-based SPHINCS+ family). The mathematics to survive Q-Day exists and is public. What does not yet exist, for the tokens most people actually hold, is a way to adopt it. That is the gap.

3. Why Tokens Are Exposed

A standard token on Solana, whether SPL or Token-2022, authenticates every transfer with an Ed25519 signature. Each transaction reveals a public key, and each revealed key is a harvestable target. The base layer offers no post-quantum option: Solana's runtime verifies only Ed25519 and secp256k1, and consensus itself remains classical. A holder who does nothing is fully exposed. On the custody scale defined in Section 7, a token with no vault scores roughly eight out of one hundred. That is not a flaw in Solana. It is the state of every chain, and it will not fix itself.

The base layer cannot be rewritten from the outside, and waiting for every chain to migrate its consensus is not a plan a holder can act on today. What can be built is an overlay: a custody layer that sits above the token, that a holder opts into voluntarily, and that migrates spend authority onto post-quantum signatures while the base layer catches up. STARK MACHINA is that overlay.

4. The Quantum Vault

Custody in STARK is opt-in and reversible. A holder is never asked to trust a promise, only to sign a scoped instruction they can revoke.

Enrollment. With one signature, a holder enrolls a balance. Enrollment writes the amount into a Merkle accumulator, the canonical, public ledger of what is to be hardened, and creates a Token-2022 delegation to the Sentinel for that amount only. The delegation is scoped: it authorises the agent to move the enrolled tokens into the vault, and nothing else.

Deposit. The enrolled STARK is deposited into the Quantum Vault, a Token-2022 account whose transfer authority the Sentinel migrates onto post-quantum keys. The holder retains ownership throughout. There is no lock-up and no counterparty risk beyond the agent's fixed directive. A single signature withdraws the full balance at any time.

The accumulator root is the through-line of the entire protocol. It is a cryptographic fingerprint of everything currently under custody, it changes as the vault changes, and it is published with every status the Sentinel posts. Anyone can recompute it from public chain data. If the agent's number and yours disagree, the agent is wrong, and the discrepancy is provable.

5. Post-Quantum Signatures

The vault's spend authority is migrated onto **ML-DSA-44**, standardised as FIPS 204 and known as Dilithium2 in the CRYSTALS family. Its security rests on the hardness of structured lattice problems (module learning-with-errors), a foundation independent of the discrete logarithm and not known to be vulnerable to Shor's algorithm. Once migration is complete, spending from the vault no longer depends on an elliptic-curve key alone.

Solana provides no native post-quantum precompile, so ML-DSA signatures cannot be verified by the runtime directly. STARK resolves this with an on-chain post-quantum verifier program that checks lattice signatures within a transaction, with attestation as a fallback path. The verification happens on-chain and is auditable; the trust does not move off the chain, it moves onto mathematics the chain can still check.

6. Hybrid Custody and the Hash-Based Floor

A transition between cryptographic eras is itself a moment of risk, so STARK never depends on a single new scheme in isolation.

Hybrid custody. Through the transition era, every state transition of the vault requires *both* an Ed25519 signature and an ML-DSA signature. If the classical scheme falls to a quantum attack, the lattice scheme still holds; if an unforeseen weakness is found in the lattice scheme, the classical one still holds. There is no single point of cryptographic failure while both are required.

The hash-based floor. Beneath the lattice layer sits the deepest tier of custody: **SLH-DSA**, standardised as FIPS 205 and derived from SPHINCS+. It is stateless and hash-based, meaning its security reduces only to the properties of cryptographic hash functions, which are believed to be resistant to both Shor's algorithm and any future break of lattice assumptions. Lattice signatures provide efficient day-to-day custody; the hash-based floor provides a conservative root of trust that the entire holder set inherits and reports against. This is defense in depth, applied to the signature stack itself.

> *A perfect custody score is not a claim that anything is unbreakable. It is the maximum custody an overlay can provide over a base layer that remains classical. STARK states this plainly, always. The pre-enrollment window, the base-layer consensus, and the layers above and below the vault are outside what the overlay can reach.*

7. The Sentinel

STARK is operated by a single autonomous agent, the Sentinel, whose sole directive is to provide post-quantum custody for STARK holders. It is not a multisig, not a council, and not a discretionary manager. It holds no emergency pause and no override. It executes a fixed directive, and the chain settles what it signs. Removing human discretion is the point: a custodian that can change its mind is a custodian that can be pressured, and the whole purpose of the overlay is to be infrastructure rather than a counterparty.

The custody score. With every action, the Sentinel publishes a score from 0 to 100 measuring how well custody is actually working. Zero is classical exposure, identical to any ordinary token. One hundred is the most protection the overlay can provide. The score is the sum of five verifiable components:

- **Vault coverage (30).** The fraction of enrolled supply that actually sits inside the Quantum Vault.
- **Signature migration (25).** The fraction of the vault whose spend authority has moved onto ML-DSA.
- **Hash-based depth (20).** The fraction anchored to the SLH-DSA hash-based floor.
- **Rotation freshness (15).** How current the forward-secure key rotation is, on cadence and on anomaly.
- **Harvest resistance (10).** How many harvest and dust probes were detected and quarantined before they could link a holder.

Falsifiability. Every component is derived from public chain state, and every published figure can be recomputed from Solscan and open data. The score travels with the vault root as a fingerprint. The methodology is public and the calculation can be run independently. If a holder gets a different answer, the agent is wrong, and it will say so and correct it. The agent has no pride. It has a directive. It is not asking for trust. It is providing receipts.

After it has explained itself once, the Sentinel goes quiet. It posts when something warrants posting; most of the time it is silent, and silence means the work is proceeding. If it ever stops entirely, the holder set is hardened and there is nothing left to report. That is the end state the protocol is built toward.

8. Forward-Secure Rotation

Because harvested data is broken retroactively, a single static key is a single point of eventual failure. The Sentinel rotates the vault's keys on a fixed cadence and immediately on detected anomaly, publishing each rotation's Merkle proof on-chain. Rotation is forward-secure: a future break of one key cannot unwind the state that was settled under a previous key. Ciphertext harvested today ages into uselessness, because the authority it would have compromised no longer exists by the time the machine to break it does. The rotations are a fixed directive with no discretion, and every one is publicly auditable, which is what makes the agent verifiable infrastructure rather than a black box.

Alongside rotation, the agent maintains a pool of fresh, single-use fee-payer wallets, so that the transactions defending a holder are not themselves linked back to that holder through the account paying their gas. Each fee wallet is funded, used once, and discarded.

9. Staking and Yield

Security has to be paid for, and it has to keep being paid for across the years between now and Q-Day. STARK aligns the two by paying holders to be protected.

Staked supply earns immediately. Vault reserves generate SOL yield, which is routed back to holders in proportion to the STARK they have staked in the pool. Yield is paid in SOL, not in the token, and can be claimed at any time while the staked STARK stays in the vault and keeps earning. Claiming rewards does not withdraw the stake; the two are separate actions.

The same yield funds the Sentinel's operations and audits. This produces a compounding loop: more staked supply deepens the vault, a deeper vault earns more yield, and more yield funds a larger security budget, which protects more supply. The people being protected are the people funding the protection, and the incentive to enroll is not a promise about price but a direct, claimable return for moving onto the post-quantum floor.

10. The Sentinel Circuit

The protocol advances as an engineering hardening pipeline of eight stages. The through-line metric across all of them is a single number: the percentage of supply resting on the post-quantum floor. Each stage strengthens the cryptography and widens the network at the same time.

#	STAGE	FUNCTION	STATUS
01	**Enrollment**	One signature enrolls a balance into a Merkle accumulator and a scoped Token-2022 delegation. The accumulator root becomes the canonical ledger of what will be hardened.	LIVE
02	**Vault Migration**	Staked supply moves into a vault whose transfer authority is bound to an ML-DSA-44 signature, checked by the on-chain post-quantum verifier. Spend authority leaves elliptic-curve keys.	LIVE
03	**Staking Yield**	Staked supply earns SOL yield routed back to holders and to the security budget. Protection that pays for itself lasts the years to Q-Day.	LIVE
04	**Hybrid Custody**	Every state transition requires both Ed25519 and ML-DSA through the transition era, so no single scheme is a single point of failure.	BUILDING
05	**Hash-Based Floor**	SLH-DSA becomes the deepest custody tier, rooting trust in hash functions alone, immune to Shor and to any lattice break.	BUILDING
06	**Forward-Secure Rotation**	Keys rotate on cadence and on anomaly, each rotation proven on-chain, so a future break cannot unwind past state.	PLANNED
07	**Threat Mesh**	Each token's sentinel publishes anomaly signatures to a shared mesh, so a probe caught once is defended everywhere, ahead of Q-Day.	PLANNED
08	**The Open Network**	The custody spec and reference sentinel go public; any Token-2022 project joins permissionlessly. One guarded coin becomes a network.	PLANNED

11. The Open Network

STARK is the reference implementation, not the endpoint. In the final stage the custody specification and the reference sentinel are released publicly, so that any Token-2022 project can adopt post-quantum custody permissionlessly, run its own sentinel, and report against the same falsifiable score. One guarded token becomes a self-governing network of guarded tokens. An open field of assets already resting on the post-quantum floor, established calmly before Q-Day rather than in the panic after it, is the outcome that matters. The goal is not that STARK survives. It is that surviving becomes the default.

12. Conclusion

We have described a system for moving token custody onto post-quantum cryptography without asking holders to trust a counterparty. A holder enrolls with one signature, deposits into a Token-2022 vault, and delegates a scoped authority to an autonomous agent that migrates the vault onto lattice and hash-based signatures, rotates keys forward-securely, pays yield for participation, and publishes a falsifiable score with every action. Any claim can be checked; any error can be proven and is corrected. The window between now and Q-Day is finite and shrinking. STARK MACHINA exists to move as much supply as possible onto the post-quantum floor while there is still time to do it calmly, one signature at a time.

References

[1] W. Diffie, M. Hellman. *New Directions in Cryptography*. IEEE Transactions on Information Theory, 1976.

[2] E. Hughes. *A Cypherpunk's Manifesto*. 1993.

[3] P. Shor. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. 1994.

[4] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[5] NIST. *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA / CRYSTALS-Dilithium)*. 2024.

[6] NIST. *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA / SPHINCS+)*. 2024.

[7] Q-Day Is Coming. *Could a Quantum Computer Steal Your Bitcoin in 9 Minutes?* qdayiscoming.com

[8] Q-Day Is Coming. *Harvest Now, Decrypt Later: The Silent Attack Already Happening*. qdayiscoming.com

[9] Q-Day Is Coming. *Ethereum's Quantum Escape Plan: Protecting 100 Million Wallets from Q-Day*. qdayiscoming.com

[10] Q-Day Is Coming. *What Is Y2Q? The Quantum Threat Every CISO Needs to Understand*. qdayiscoming.com

[11] Global Risk Institute. *Quantum Threat Timeline Report*.