H33 Adds Post-Quantum Privacy to Bitcoin

Institutional Bitcoin holders can now prove compliance, reserves, and custody without revealing wallets, balances, or transaction history.

H33 Logo

RIVERVIEW, FL, UNITED STATES, May 21, 2026 /EINPresswire.com/ -- H33.ai, Inc. today announced the deployment of post-quantum privacy infrastructure for Bitcoin, making H33 the first platform to anchor STARK-based privacy attestations directly on the Bitcoin blockchain via Taproot witness data. The same infrastructure is already portable across Ethereum, Solana, Zcash, and additional blockchain environments using chain-native storage primitives.

> Bitcoin made verification public and institutional privacy nearly impossible, H33 allows institutions to prove reserves, compliance, and custody without exposing wallets or operational structure”
>
> *Eric Beans*

The infrastructure enables institutional Bitcoin holders — including ETF custodians, corporate treasuries, and regulated financial institutions — to cryptographically prove compliance, reserves, and custody status without revealing wallet addresses, UTXO composition, or balance information.

THE PROBLEM

Bitcoin's transparent ledger creates a fundamental conflict for institutional adoption. ETF custodians must demonstrate reserve adequacy to regulators, but doing so exposes their complete wallet infrastructure. Corporate treasuries must prove compliance, but every proof reveals their holdings to competitors. Mining operations must report output, but reporting discloses operational structure.

Existing privacy approaches for Bitcoin — mixers, CoinJoins, and layer-2 networks — either lack regulatory compatibility or rely on elliptic curve cryptography that quantum computers will break.

THE SOLUTION

H33's Bitcoin privacy infrastructure uses zero-knowledge STARK proofs to verify claims about

Bitcoin holdings and transactions without revealing the underlying data. The proofs are:

- Post-quantum: Built entirely on hash-based cryptography (SHA3-256, Poseidon). No elliptic curves. No pairings. No quantum expiration date.

- Independently verifiable: Any regulator, auditor, or counterparty can verify any attestation using the open-source HATS verifier. No API key. No vendor trust. No platform dependency.

- Permanently anchored: A single 32-byte commitment — always exactly 32 bytes, by design — is embedded in Bitcoin's native Taproot witness data. No images. No tokens. No arbitrary data. The attestation is as permanent and as minimal as a Bitcoin transaction allows.

H33.ai - The World's First Complete Quantum-Proof Security Platform

- Three-family attested: Every attestation is signed by three independent post-quantum signature families — ML-DSA-65 (MLWE lattice), FALCON-512 (NTRU lattice), and SLH-DSA-128f (hash-based) — under the H33-74 attestation standard. Forgery requires simultaneously breaking all three mathematical hardness assumptions.

HOW IT WORKS

A STARK proof is generated that verifies a claim — for example, "this custodian holds at least 10,000 BTC" or "this transaction satisfies OFAC sanctions screening." The proof is distilled into a 32-byte commitment, signed by three post-quantum signature families, and anchored to Bitcoin via a Taproot witness envelope. The full proof is stored off-chain and retrievable for independent verification.

The anchoring uses Bitcoin's native Taproot (SegWit v1) witness data structure. The on-chain footprint is exactly 32 bytes — a fixed-size cryptographic commitment that cannot carry images, tokens, or arbitrary content. This constraint is architectural, not incidental. The system was designed to produce the smallest possible on-chain footprint for the strongest possible off-chain proof.

No modification to the Bitcoin protocol is required. No fork. No sidechain. No layer-2 dependency.

INSTITUTIONAL USE CASES

- ETF Custody Verification: Custodians prove reserve adequacy to regulators without revealing wallet addresses or UTXO distribution. The proof is permanently anchored on Bitcoin and verifiable by any authorized party.

- Corporate Treasury Compliance: Public companies holding Bitcoin on their balance sheet prove regulatory compliance without exposing their complete holdings to competitors or the public.

- Mining Operation Attestation: Mining operations prove hash rate output, energy sourcing, and production volume without revealing operational infrastructure or competitive positioning.

- OTC Transaction Compliance: Over-the-counter trading desks prove transaction legitimacy and sanctions compliance without revealing counterparty identities or trade details.

- Provable Reserves: Any entity holding Bitcoin can prove solvency and reserve adequacy without a full on-chain audit that exposes their entire wallet structure.

MULTI-CHAIN INFRASTRUCTURE

The Bitcoin deployment is part of H33's broader chain-agnostic privacy and attestation infrastructure, already deployed across Bitcoin, Ethereum, Solana, and Zcash.

The underlying STARK proof system and H33-74 attestation layer remain identical across every network. Only the anchoring mechanism changes:

- Bitcoin: Taproot witness envelopes
- Ethereum / L2s: calldata commitments
- Solana: PDA account anchoring
- Zcash: memo field commitments

This allows the same post-quantum proof to move between chains without modifying the proof itself.

"The cryptography is portable. The proof is portable. The attestation is portable," said Beans. "Only the storage surface changes between chains. That is the difference between infrastructure and an application-specific privacy tool."

Because the proof system is chain-independent, institutions can standardize on a single verification architecture across multiple blockchain environments instead of deploying separate privacy systems per network.

POST-QUANTUM SURVIVABILITY

Unlike all existing blockchain privacy solutions — which rely on elliptic curve cryptography

vulnerable to Shor's algorithm — H33's STARK proofs use only hash-based commitments and arithmetic over the Goldilocks prime field. The proofs carry no quantum expiration date.

This is particularly significant for Bitcoin, where transaction history is permanent. Privacy attestations anchored today must remain valid for decades. Classical cryptographic assumptions will not hold that long. H33's post-quantum construction ensures the attestation is as durable as the Bitcoin blockchain itself.

INDEPENDENT VERIFICATION

H33 has published an open-source governance bundle verifier (HATS Verifier) that enables any party to independently verify attestations without trusting H33, the attesting institution, or any intermediary. The verifier is available at github.com/H33ai-postquantum/hats-verifier and can be installed via cargo install hats-verifier.

The verification architecture operates at three levels:

- Fast verification (under 400ms): Confirm the 32-byte commitment exists in a Bitcoin transaction.
- Standard verification (under 5ms): Verify the H33-74 post-quantum attestation signatures.
- Full mathematical verification (under 100ms): Retrieve and verify the complete STARK proof. Trust only mathematics.

WHY THIS MATTERS NOW

Bitcoin has become institutional collateral, not just a speculative asset. ETFs, public companies, custodians, miners, and sovereign buyers increasingly need to prove what they hold, what they control, and whether they are compliant — without turning their treasury into public intelligence.

H33 gives Bitcoin institutions a third option:

Not secrecy without proof. Not transparency without privacy. Cryptographic proof without exposure.

This turns Bitcoin from a fully transparent settlement layer into a privacy-compatible institutional proof layer — without changing Bitcoin, weakening compliance, or asking anyone to trust H33.

The result is simple: institutions can now prove the truth about Bitcoin positions without revealing the positions themselves.

AVAILABILITY

H33's Bitcoin privacy infrastructure is available immediately for institutional customers. The Taproot anchoring module supports both mainnet and testnet, with OP_RETURN as a legacy fallback. API access is available through h33.ai.

ABOUT H33

H33.ai, Inc. builds post-quantum trust infrastructure for institutions. The H33 platform includes five proprietary cryptographic engines (BFV, CKKS, TFHE, STARK, and three-family PQ signatures), the H33-74 attestation standard, and the HATS governance verification framework. H33 holds seven patents pending with over 250 patent claims covering post-quantum attestation, FHE computation verification, and cryptographic distillation.

For more information, visit h33.ai/bitcoin-privacy.

Media Contact:
Eric Beans, CEO
H33.ai, Inc.
support@h33.ai
h33.ai

Eric D Beans
H33.ai, Inc.
email us here
+1 813-464-0945
Visit us on social media:
LinkedIn
YouTube
X
