H33.ai Distills Three Post-Quantum Signature Families Into 74 Bytes — and Anchors Them to Bitcoin

The Same 74 Bytes That Quantum-Proofs Bitcoin Quantum-Proofs Everything Else — Without Touching a Single Line of Existing Infrastructure

H33 Logo

RIVERVIEW, FL, UNITED STATES, April 15, 2026 /EINPresswire.com/ -- H33.ai, Inc. today announced the filing of a United States patent application covering H33-74 — the commercial name for the Canonical Commitment Substrate, a cryptographic primitive that distills three independent post-quantum signature families from 21,063 bytes to a permanent 74-byte footprint — and simultaneously released the accompanying technical whitepaper and verified the construction on the Bitcoin mainnet. The announcement arrives two weeks after new research demonstrated that future quantum computers could threaten Bitcoin's cryptographic foundations with far fewer resources than previously assumed, reigniting urgent debate across the cryptocurrency, enterprise security, and financial infrastructure communities about the viability of existing cryptographic protections.

> “Post-quantum keys will get heavier, and H33-Substrate will stay 74 bytes forever. Post-quantum cryptography was supposed to make everything heavy and slow. H33 makes it lighter and faster than today.”
>
> - *Eric Beans, CEO, H33.ai*

What Was Filed and Verified Today

H33-74 is a fixed-width cryptographic primitive that simultaneously commits to any computation result through three independent post-quantum signature algorithms: ML-DSA-65 (NIST FIPS 204), FALCON+ (Draft FIPS 206), and SLH-DSA-SHA2-128f (NIST FIPS 205). These three algorithms rest on three mutually disjoint mathematical hardness assumptions — Module Learning With Errors, Short Integer Solution over NTRU lattices, and SHA3-256 pre-image resistance respectively. The construction's formal security level is bounded by its weakest family at NIST Level 1 — a deliberate design choice that prioritizes assumption diversity over security level parity. Forging any H33-74 attestation requires simultaneously breaking all three hardness assumptions across all three independent algorithm families. No known cryptanalytic advance against any single

family affects the other two.

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

The construction produces a 58-byte substrate commitment and a 42-byte compact receipt. The 32-byte hash of the substrate anchors on-chain; the 42-byte receipt stores off-chain. The combined persistent footprint is 74 bytes — permanently. As quantum computers grow more powerful and post-quantum signature schemes adopt heavier parameter sets, the on-chain and off-chain footprint of every H33-74 attestation remains exactly 74 bytes.

On April 14, 2026, H33.ai anchored the first H33-74 attestation to the Bitcoin mainnet in a single standard transaction containing both a Taproot P2TR output and an OP_RETURN output, confirming both supported anchoring methods simultaneously. The transaction was broadcast through the public Bitcoin mempool using Bitcoin Core 28.0 with no modifications, no private relay service, and no soft fork. Transaction ID

7f8d9ef2d5625d7e3acbc269daac21087ce6b7d77f8e4ec369aabdcdb028b4a7 is independently verifiable by any Bitcoin full node worldwide.

The Architectural Consequence for Bitcoin

The Taproot key-path tweak anchoring method adds zero marginal transaction weight and is indistinguishable from any other Taproot spend. No Bitcoin consensus rules are modified. No new opcodes are introduced. No validator software requires updating. No soft fork is needed. H33-74 composes with a capability Bitcoin has possessed since the activation of Taproot at block 709,632 in November 2021 — the capacity to embed fixed-width data in transaction outputs — and surfaces that capability as a universal post-quantum attestation anchor for arbitrary computation across every domain.

This is not a claim about Bitcoin's design intent. It is an observation about architectural sufficiency. Bitcoin supplies global immutability, permissionless timestamping, and a fifteen-year track record of adversarial resilience. H33-74 supplies three-family post-quantum signature security, computation-type domain separation through an append-only registry, and batched Merkle aggregation that amortizes the per-result signing cost as O(1/N). The composition produces, as a structural consequence, a cryptographic attestation infrastructure whose trust properties are inherited from the Bitcoin ledger's own consensus security.

Unbounded Scale at Fixed Cost

H33-74 supports unbounded Merkle aggregation. A single Bitcoin transaction anchoring one 74-

byte root can commit to a batch of N attestations where N is bounded only by available memory — including batches exceeding one quadrillion individual computation results. Per-leaf inclusion proofs scale as O(log N). The per-result attestation cost amortizes to microseconds at batch sizes achievable in production. At a sustained production throughput of 2,175,029 attestations per second on a 192-vCPU AWS Graviton4 instance, and at commodity cloud pricing of approximately $2.30 per instance-hour, the hardware cost per attested computation is approximately $3.8 × 10⁻¹⁰.

Applications Across Every Domain

H33-74 is computation-agnostic. The same 74-byte primitive that attests a Bitcoin UTXO also attests an HTTP API response, an AI inference output, a captured media frame, a legal evidence chain of custody, a medical record modification, a tokenized real-world asset issuance, and a federated machine-learning model weight exchange. Eight applications are implemented and described in the accompanying whitepaper. Each assigns a distinct computation type byte from an append-only domain separation registry, ensuring that attestations produced in one domain cannot be replayed as valid attestations in another.
The construction addresses directly the performance problem that has blocked post-quantum adoption at scale. Prior post-quantum signature schemes produced signatures orders of magnitude larger than the systems they were designed to protect — a single SLH-DSA signature is 17,088 bytes, a three-family bundle totals 21,063 bytes. H33-74 does not compress these signatures. It commits to them through a fixed-width primitive, stores them off-chain indexed by a 42-byte receipt pointer, and places only 32 bytes on any ledger or in any storage-constrained environment. The signatures remain retrievable and fully verifiable on demand.

Commercial Deployment and Pricing

The reference commercial implementation ships as a customer-hosted binary that runs entirely on customer-owned infrastructure inside a Trusted Execution Environment. No H33-74 operation requires a network call to H33.ai infrastructure after an initial one-time key provisioning event. Billing is metered through the Bitcoin blockchain itself: every H33-74 anchor is a public on-chain commitment observable by both the vendor and the customer from the same authoritative immutable ledger, structurally eliminating billing disputes.

The commercial rate is determined by cumulative global daily volume across all customers — not by any individual customer's usage. The launch rate is $0.025 per mint. A free evaluation tier of 10,000 mints per month is available to any developer with an email address, with no credit card required.

Publication and Verification

The technical whitepaper, entitled "The Canonical Commitment Substrate: A Post-Quantum Primitive for Computation-Result Attestation," is available at https://h33.ai/h33-74/whitepaper/

About H33.ai, Inc.

H33.ai, Inc. is a post-quantum security infrastructure company headquartered in Riverview, Florida. The company develops cryptographic primitives, attestation infrastructure, and compliance tooling for enterprise, financial services, healthcare, , and blockchain applications.

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

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