H33 Demonstrates Post-Quantum 'Proof Layer' for Tokenized Assets — Enabling Encrypted, Verifiable Financial Instruments

Six patents pending. Three directly solve the missing layer in tokenization: provable truth without exposure.

H33 Logo

RIVERVIEW, FL, UNITED STATES, April 30, 2026 /EINPresswire.com/ -- As financial institutions accelerate the tokenization of real-world assets, a fundamental limitation remains unresolved: how to verify what has occurred to an asset without relying on the system that processed it.

H33.ai today demonstrated a production implementation designed to address that problem.

> Without attestation from creation, tokenization is premature. We provide the speed, scale, and a full chain of proof - who, what, when, why, and how - that FHE alone can't deliver."
>
> *-Eric Beans CEO H33.ai, Inc.*

In a live execution, a simulated $10 million U.S. Treasury bond was processed through a pipeline in which the underlying data was never exposed in plaintext—at any stage. Compliance evaluation, scoring, and verification were performed directly on encrypted values using fully homomorphic encryption. The resulting computation was signed under three independent NIST-standardized post-quantum signature families and anchored simultaneously across Bitcoin, Ethereum, Solana, and Chainlink.

The chain link in that pipeline is the cross-chain attestation anchor.

Here's what each chain does:

Bitcoin — permanent timestamped proof. The 32-byte H33-74 commitment goes into a Taproot witness or OP_RETURN. Bitcoin is the most immutable ledger -once confirmed, that attestation is permanent. This is what the Bonds demo does live at h33.ai/bitbonds/demo/.

Ethereum — smart contract verifiability. The commitment is written to an EVM contract where

other smart contracts can read and verify it on-chain. This matters for DeFi, RWA tokenization, and any Ethereum-native compliance workflow that needs to check "was this bond attested?"

Solana - high-speed, low-cost anchoring via memo instruction. Your Solana demo does this live. Solana's sub-second finality means the attestation is verifiable almost instantly. This matters for trading desks and high-frequency settlement.

Chainlink - this is the bridge layer. Chainlink doesn't store the attestation itself. It makes the attestation available to any chain Chainlink connects to. Chainlink's oracle network reads the H33-74 commitment from one chain and makes it queryable from others. This means:

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

- A smart contract on Polygon can verify the bond attestation anchored on Bitcoin
- An Avalanche DeFi protocol can check the compliance proof anchored on Ethereum
- Any Chainlink-connected chain gets access to the attestation without H33 needing to anchor to every chain individually

The architecture:

Bond data (encrypted, never plaintext)
□
□□□ FHE: BFV encrypts bond fields
□□□ FHE: TFHE runs encrypted compliance check
□□□ H33-74: 74-byte commitment (SHA3-256 + 3 PQ signatures)
□
□□□ Anchor to Bitcoin (permanent proof, Taproot)
□□□ Anchor to Ethereum (smart contract verifiable)
□□□ Anchor to Solana (fast finality, memo instruction)
□□□ Anchor to Chainlink (cross-chain oracle distribution)
□
□□□ Any Chainlink-connected chain can verify
(Polygon, Avalanche, Arbitrum, Base, etc.)

Why all four? Different counterparties live on different chains. The bond issuer might be on Ethereum. The custodian might verify on Solana. The regulator might only trust Bitcoin's

immutability. The secondary market might be on Polygon via Chainlink. Anchoring to all four means the attestation is verifiable wherever the counterparty operates - without anyone ever seeing the bond data in plaintext.

The key point: the H33-74 commitment is the same 32 bytes on every chain. One computation, one attestation, four anchors. The bond data never leaves FHE encryption. The chains prove the attestation existed at a specific time - they don't know what was attested.

Each signature is independently verifiable without access to the underlying data. At no point is the financial data exposed. From Representation to Verification Tokenization has largely focused on representation- how an asset is expressed digitally. Whether as a token on a ledger, a smart contract reference, or an off-chain document, the representation alone does not establish what actually occurred.

In practice, tokenized assets continue to rely on the same trust assumptions as traditional systems: internal controls, audit processes, and reliance on privileged access to sensitive data. Verification remains dependent on institutions rather than cryptographic proof.

H33 introduces a different model: a cryptographic proof layer that binds the identity of an asset, the computation performed on it, and the resulting outcome into a single, portable, post-quantum verifiable artifact.

This artifact captures four elements:

-the identity of the asset, bound at creation through H33-Upstream chain of custody
-the evaluation process, executed with cryptographic commitments
-the computation itself, deterministic and reproducible
-the resulting outcome, committed under multiple post-quantum signature schemes without revealing inputs

System Execution

The BitBond demonstration reflects a full lifecycle for a tokenizable financial instrument.

Data enters the H33-Upstream boundary and is immediately encrypted using fully homomorphic encryption. From that point forward, the data does not exist as coherent plaintext outside the originating environment. The raw data remains inaccessible without the originating key, which H33 does not hold.
Compliance functions-including OFAC screening, KYC verification, accredited investor validation, and AML checks-are executed directly on encrypted values.

No intermediary, vendor, or operator has access to the underlying financial data.

A deterministic cryptographic fingerprint is then computed over the ciphertext, encrypted state, and execution environment. This produces a binding commitment that links the data, the computation, and the context in which it occurred. This fingerprint is encrypted independently of the homomorphic key hierarchy, ensuring separation between computation and verification. As a result, the party executing the computation cannot access verification data, and the verifier cannot access the computation itself.

The resulting commitment is signed under three independent post-quantum signature families:

ML-DSA (lattice-based)
FALCON (NTRU lattice)
SLH-DSA (hash-based)
The full signature set-approximately 21 kilobytes for (NIST 1) to 35 kilobytes (NIST 5)-is preserved intact on Cachee.ai, a post quantum caching company. Rather than compressing this data, the system distills it into a constant-size commitment and retrieval handle: a 58-byte canonical substrate and a 74-byte persistent anchor. The anchor does not contain the proof. It binds to it.

The complete verification state remains intact and independently retrievable. The blockchain stores only the commitment; the full proof remains off-chain and cryptographically bound to that commitment. Verification reconstructs the proof from the bound state rather than from the chain itself.

Multi-Network Verification

The commitment is anchored across multiple independent networks:

-Bitcoin provides neutral, immutable timestamping
-Ethereum enables programmable verification
Solana provides high-throughput validation
-Chainlink enables external distribution and cross-system verification
-The same proof verifies identically across all networks without modification or translation.

Architecture

The system is composed of three integrated components.

-H33-Upstream establishes cryptographic chain of custody at the moment of data creation, binding origin, execution environment, and lineage.
-H33-74 produces a fixed-width post-quantum attestation primitive that commits to computation results without revealing inputs.
-H33-TFHE provides encrypted decisioning and routing across heterogeneous cryptographic engines, committing both the computation result and the decision process to a verifiable, post-

quantum signed record.

Together, these components create a continuous verification chain:
asset creation encrypted processing compliance evaluation result commitment multi-chain anchoring independent verification

At no point is the underlying data exposed.

Extension to Cyber Insurance

The same architecture underpins HATS, H33's continuous verification system for cyber insurance.
HATS produces cryptographically attested evidence of security controls-including MFA, endpoint protection, backups, patching, and network segmentation-for underwriting and claims evaluation.

In the event of a claim, the system reconstructs the verified state at the time of the incident using attested records rather than logs or post-incident analysis.
Across both financial instruments and insurance policies, the underlying question is consistent: whether the state of a system can be proven at the moment it matters, without reliance on trusted intermediaries.

Implications

This model enables:
-tokenized assets to demonstrate compliance without exposing sensitive data
-institutions to validate state without sharing underlying information
-regulators to verify outcomes without accessing raw inputs
-insurers to evaluate claims based on attested evidence rather than reconstructed logs
-long-term custody models based on chained, verifiable attestations

Performance

-The system is currently operating with the following characteristics:
-42 microseconds per attestation
-2.2 million operations per second per node
-FHE routing latency under 500 nanoseconds
-CKKS inference throughput of 1,574 transactions per second
-TFHE decision throughput of 768 transactions per second
-Attestation substrate: 58 bytes
-Anchor: 74 bytes (constant size)
-On-chain footprint: 32 bytes

Conclusion

Tokenization established digital representation. H33 introduces verifiable execution.

About H33.ai

H33.ai develops post-quantum cryptographic infrastructure for secure computation, verification, and data protection. The platform integrates fully homomorphic encryption, post-quantum signatures, and attestation systems into a unified architecture designed to eliminate plaintext exposure while enabling independent verification.

Six patents pending. Over 250 claims. SOC 2 Type II and ISO 27001 compliant. Available on AWS Marketplace.

Media Contact
media@h33.ai
https://h33.ai

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