VeritasChain Standards Organization (VSO) Announces World's First Regulator-Operated Audit Trail Verification PoC

VeritasChain Standards Organization to demonstrate real-time Merkle proof verification enabling regulators to independently validate algorithmic trading logs.

Logo of the VeritasChain Standards Organization (VSO), a neutral standards body developing cryptographic audit and provenance frameworks for AI systems.

TOKYO, JAPAN, January 26, 2026 /EINPresswire.com/ -- Overview

VeritasChain Standards Organization (VSO) today announces the forthcoming implementation of a Real-Time VCP Supervision Node Proof-of-Concept (PoC), a supervisory infrastructure enabling financial regulatory authorities to independently verify the integrity of algorithmic trading audit trails through cryptographic Merkle proofs and third-party anchoring.

Independent research conducted by multiple AI research systems across supervisory technology, regulatory technology, cryptographic transparency logs, and commercial market surveillance products identified no direct precedent for this capability in published literature, commercial products, or regulatory authority implementations.

To the best of available knowledge, this PoC represents the first publicly documented reference implementation of a regulator-operated node for Merkle proof-based verification of financial trading logs with third-party anchoring.

 The Verification Problem

Current regulatory frameworks for algorithmic trading, including MiFID II, the EU AI Act, DORA, and SEC Rule 17a-4, mandate comprehensive audit trails. However, a fundamental limitation persists: regulatory authorities must largely trust that business logs submitted by regulated entities have not been tampered with, selectively deleted, or retrospectively modified.

> We are building a regulator-side supervision node that verifies anchored Merkle proofs in near real time, so authorities can confirm trading log integrity without trusting self-reported records."
>
> *Tokachi Kamimura, Executive Director, VeritasChain Standards Organization*

This trust-based paradigm creates an information asymmetry wherein the regulated entity possesses full control over evidence while the regulator possesses limited means of independent verification.

The Real-Time VCP Supervision Node addresses this asymmetry by enabling a paradigm shift from trust-based acceptance to mathematical verification, embodying the principle of Verify, Don't Trust.

 Technical Innovation

The PoC introduces a novel architecture with three key participants. Regulated entities generate VCP-compliant audit trails with cryptographic integrity guarantees including hash chains, digital signatures, and Merkle trees. Third-party anchoring services, such as RFC 3161 Timestamp Authorities or public blockchains, provide tamper-evident temporal commitments independent of all parties. Regulatory authorities operate their own supervision nodes that receive anchored Merkle roots and can independently verify any event's inclusion, completeness, and temporal integrity without relying on the submitting entity's infrastructure.

This tripartite architecture eliminates the single point of trust inherent in current regulatory reporting mechanisms.

The supervision node will demonstrate five core capabilities. First, independent verification allowing regulators to validate trading logs using only submitted VCP events, Merkle proofs, and third-party anchor references. Second, tampering detection identifying event modification, deletion, insertion, or timestamp manipulation. Third, multi-entity supervision monitoring multiple regulated entities through a unified dashboard with real-time integrity status. Fourth, on-demand verification enabling supervisory authorities to request Merkle inclusion proof for any arbitrary event and verify within seconds. Fifth, regulatory report generation aligned with DORA incident reporting frameworks and FCA evidence submission requirements.

 Research Foundation

Prior to PoC development, comprehensive competitive analysis was conducted through independent research by multiple AI research systems. The investigation spanned supervisory technology implementations by central banks and financial regulators, cryptographic transparency log architectures including Certificate Transparency and SCITT, commercial market surveillance products from major vendors, academic literature, standards body publications, and patent databases.

The research evaluated four distinct assertions. Assertion A examined whether a regulator-side node independently verifying third-party-anchored Merkle proofs exists. Assertion B examined whether a supervisory dashboard receiving anchored Merkle roots from multiple entities with real-time integrity visualization exists. Assertion C examined whether on-demand regulatory capability to request and verify Merkle paths for any event exists. Assertion D examined whether application to algorithmic trading and HFT logs with high-precision timestamps exists.

All four assertions were supported with appropriate qualifications, finding no publicly documented precedent matching the combined capabilities.

 Standards Alignment

The PoC is built upon VeritasChain Protocol v1.1, an open cryptographic audit trail standard submitted to the Internet Engineering Task Force as draft-kamimura-scitt-vcp, aligning with the Supply Chain Integrity, Transparency and Trust architecture.

VCP v1.1 defines a three-layer integrity architecture. Layer one provides event integrity through SHA-256 hashing and time-ordered UUIDv7 identifiers. Layer two provides collection integrity through RFC 6962 compliant Merkle trees. Layer three provides external verifiability through Ed25519 digital signatures, RFC 3161 timestamps, and mandatory external anchoring.

The PoC demonstrates compliance with regulatory requirements across ten jurisdictions including the EU, UK, US, Japan, Singapore, Hong Kong, Australia, Canada, and Switzerland, covering over sixty regulatory documents.

 Implementation Timeline

Implementation will commence when requisite conditions are satisfied. VSO welcomes engagement from financial regulatory authorities interested in SupTech innovation, central banks exploring cryptographic audit infrastructure, standards bodies contributing to audit trail standardization, and academic institutions researching transparency log applications.

 About VeritasChain Standards Organization

VeritasChain Standards Organization is a vendor-neutral standards body developing open cryptographic audit trail standards for AI-driven and algorithmic trading systems. Operating under the philosophy of Verify, Don't Trust, VSO positions the VeritasChain Protocol as AI's Flight Recorder, creating tamper-evident audit trails using hash chains, digital signatures, and Merkle trees.

 Contact Information

General Inquiries: info@veritaschain.org
Technical: technical@veritaschain.org
Regulatory Engagement: compliance@veritaschain.org
Website: https://veritaschain.org
GitHub: https://github.com/veritaschain
IETF Draft: https://datatracker.ietf.org/doc/draft-kamimura-scitt-vcp/

TOKACHI KAMIMURA
VeritasChain Co., Ltd.
kamimura@veritaschain.org
Visit us on social media:
LinkedIn
Bluesky
Facebook
YouTube
X
Other
