ISO/TC 68 JWG 7
AI in Financial Services

Document Type: Technical Input (Non-Normative)
Date: 2025-12-22
Document ID: VSO-INPUT-TC68-JWG7-001

Technical Input: Verifiable Logging and Audit Evidence for AI-Driven Financial Systems

1. Context

The adoption of artificial intelligence and algorithmic trading systems in financial services continues to expand globally. Regulatory frameworks increasingly require comprehensive logging and record-keeping for such systems to ensure accountability, enable post-incident analysis, and support market surveillance. However, current implementations often lack mechanisms for **third-party verifiable audit evidence**—logs that can be independently validated without relying solely on the submitting party's internal controls.

2. Problem Statement

- Logging mechanisms are typically controlled by internal administrators, creating dependency on submitter integrity
- Detection of log tampering, selective omission, or retroactive modification is technically difficult
- Timestamp accuracy and clock synchronization status are often not preserved as verifiable evidence
- Independent verification by auditors, regulators, or third parties requires trust in the data provider
- Privacy-preserving approaches for audit evidence remain insufficiently addressed

3. Implementation Pattern (Non-Normative)

This section describes one possible technical pattern for verifiable logging. It is provided as an illustrative example, not as a prescriptive requirement.

- **Event-based logging:** Capturing the complete lifecycle from signal generation through order submission, execution, and position closure as discrete, typed events
- **Cryptographic chaining:** Linking each event to its predecessor via cryptographic hash, enabling detection of insertion, deletion, or modification
- **Merkle tree aggregation:** Periodic anchoring of event batches into Merkle roots for efficient bulk verification
- **Time synchronization evidence:** Recording not only timestamps but also the synchronization method and status (e.g., NTP, PTP, GPS) as part of the audit record
- **Third-party verifiability:** Enabling verification of log integrity and completeness without requiring access to internal systems or trust in the submitter
- **Privacy consideration:** Designing structures where personal identifiers can be pseudonymized or excluded while preserving cryptographic integrity

4. Relevance to ISO/TC 68 JWG 7 Technical Report

This input may inform discussions on logging, record-keeping, and audit evidence within the Technical Report on AI in Financial Services. The described pattern aligns with regulatory expectations for algorithmic trading oversight, including requirements for timestamp accuracy, complete audit trails, and independent verification capabilities. The approach is implementation-neutral and may complement existing ISO/IEC standards on AI management systems and information security controls.

5. Status and Disclaimer

- This document is provided as **non-normative technical input** for discussion purposes
- It does not propose a new standard or modification to existing standards
- It does not represent endorsement by any regulatory authority or standards body
- The described implementation pattern is illustrative; other approaches may be equally valid
- This input is submitted by VeritasChain Standards Organization (VSO) for reference only

Submitted by: VeritasChain Standards Organization (VSO) | standards@veritaschain.org | veritaschain.org