PUBLICLY DOCUMENTED WORLD-FIRST EVIDENCE REPORT

Cryptographic Audit Trail for cTrader Trading Workflows

Prior Art Research Consolidation | January 2026

CONSOLIDATED FINDING: Five independent research analyses across academic databases, open-source repositories, vendor documentation, and multilingual searches (EN/RU/TR/JA) confirm: NO publicly documented prior art exists meeting all five required criteria for cryptographic audit trails in cTrader-based trading workflows. Confidence Level: HIGH (90%+)

1. Research Overview

This report consolidates findings from five independent research analyses (Sources A-E) conducted between December 2025 and January 2026. The research examined whether any publicly documented implementation exists that meets ALL five criteria for cryptographic audit trails specifically targeting cTrader trading workflows.

Research Sources Examined:

- Academic databases: Google Scholar, IEEE Xplore, ACM Digital Library, arXiv, USENIX, SSRN
- Open-source: GitHub, GitLab (85+ targeted searches across multiple languages)
- Official documentation: Spotware cTrader API, FIX API, Open API, cAlgo references
- RegTech vendors: NICE Actimize, Nasdaq SMARTS, FIS Protegent, SteelEye, MAP FinTech
- Patent repositories: USPTO, Google Patents (1990-2025)
- Multilingual searches: English, Russian, Turkish, Japanese

2. Five Required Criteria (ALL Must Be Met)

#	Criterion	Technical Requirement
1	cTrader Platform	Specifically targets cTrader (not MT4/MT5 or generic FIX systems)
2	Cryptographic Audit	Generates cryptographically verifiable audit trails for trading events
3	Crypto Primitives	Uses hash chains, Merkle trees (RFC 6962), or digital signatures (Ed25519)
4	Public Documentation	Enables independent third-party verification with open specifications
5	Production Evidence	Demonstrates deployment in live or production-equivalent environments

3. Related Works Analysis (Consolidated)

The following table consolidates all related technologies identified across the five research analyses, showing which criteria each fails to meet:

Source	Year	Platform	Crypto Features	Public	Gaps vs Criteria

VeritasChain Protocol (VCP)	2025	MT4/MT5 (cTrader in docs only)	Ed25519, SHA-256 hash chains, RFC 6962 Merkle	Yes	FAILS #1: cTrader mentioned but no implementation
Spotware cTrader Native	2012-2025	cTrader	None - standard logging only	N/A	FAILS #2-3: No crypto primitives, admin-modifiable logs
ISAE 3402 Audit	2012	cTrader	None - procedural	Partial	FAILS #2-3: Operational controls only
Thorpe & Willis (FC 2012)	2012	Custom Exchange	Cryptographic commitments	Partial	FAILS #1,5: Not cTrader theoretical only
Crosby & Wallach	2009	Generic	Merkle history trees	Yes	FAILS #1,5: Platform-agnostic, no trading
Trillian (Google)	Active	Generic infra	RFC 6962 Merkle trees	Yes	FAILS #1,5: Not cTrader no trading integration

4. Key Findings from Independent Analyses

• **Zero cTrader implementations found:** Despite 85+ targeted searches across multiple databases and languages, no system combines cTrader + cryptographic verification + public documentation.

• **cTrader native capabilities limited:** cTrader provides MAP FinTech integration for MiFID II/EMIR reporting, but these are database-backed logs susceptible to administrator modification. No hash chains, Merkle trees, or digital signatures exist in official Spotware documentation.

• **VCP is closest but MT4/MT5 only:** The VeritasChain Protocol mentions cTrader in documentation but all production validation (ABLENET Japan, December 2025) was conducted exclusively on MT4/MT5. No cTrader-specific code, integration examples, or deployment evidence exists in any VCP repository.

• **Academic gap confirmed:** Foundational work on tamper-evident logging (Crosby & Wallach 2009, Schneier & Kelsey 1998) exists but remains platform-agnostic. Zero papers address cTrader specifically.

• **Regulatory context supports novelty:** SEC Rule 17a-4 (2022) and EU AI Act (2024) recognize cryptographic audit trails as valid compliance mechanisms, but no cTrader implementation exists.

5. Confidence Assessment

Factor	Assessment	Rationale
Search Coverage	Comprehensive	85+ searches, 5 independent analyses, multilingual (EN/RU/TR/JA)
Source Diversity	High	Academic, open-source, vendor, patent, regulatory sources examined
Null Result Consistency	100%	All 5 analyses returned consistent null results for cTrader
Closest Alternative	Disqualified	VCP (MT4/MT5 only), Aegis MQL (closed SaaS) fail criteria
Conservative Framing	Applied	"To the best of our knowledge" hedges against undocumented systems

Overall Confidence Level: HIGH (90%+)

6. Defensible Statement

"To the best of our knowledge, this is the first publicly documented and independently verifiable cryptographic audit trail implementation for cTrader-based trading workflows."

This statement is **technically defensible** based on comprehensive research across five independent analyses. The qualifier "to the best of our knowledge" appropriately acknowledges the possibility of undocumented proprietary systems while accurately representing the state of publicly accessible prior art as of January 2026.

7. Research Source Summary

ID	Type	Description	Key Finding
A	Deep Research Analysis	85+ searches, 136 citations, academic & patent analysis	Zero cTrader crypto audit prior art found (High conf.)
B	Multilingual Search	EN/RU/TR/JA searches, RegTech vendor analysis	No public verification solution for cTrader
C	Technical Analysis	GitHub, Spotware docs, VCP repository analysis	VCP MT4/MT5 only, cTrader aspirational docs only
D	Academic Research	Academic databases, related works table	No cTrader-specific papers, all partial implementations
E	Due Diligence Report	Technical deep-dive, Japanese business context	cTrader ecosystem trust-based not verification-based