AML Enforcement Architecture: A Governance-Grade Specification for Global Financial Systems

Lev Goukassian

Independent Researcher / Ternary Logic Architecture
Santa Monica, California, USA

ORCID: 0009-0006-5966-1243

leogouk@gmail.com

Abstract

The global Anti-Money Laundering (AML) framework currently operates on a bivalent (binary) logic of "Allow" or "Deny," creating a structural inability to manage economic actions under epistemic uncertainty. This architecture forces high-ambiguity transactions into a permissive state to maintain liquidity, resulting in an "interdiction gap" where illicit funds are identified only after settlement via post-hoc Suspicious Activity Reports (SARs). This paper proposes **Ternary Logic (TL)**, a triadic state-machine architecture (+1 Proceed, 0 Epistemic Hold, -1 Refuse) that enforces "No Log = No Action" constraints at the protocol level. We define the *Epistemic Hold* as a deterministic, time-bounded state that converts unbounded probabilistic regulatory risk into bounded, measurable latency. The technical specification introduces a **Dual-Lane Latency** architecture to decouple inference (≤2ms) from cryptographic anchoring (≤500ms), and utilizes **Merkle-batched anchoring** to achieve O(1) verification complexity per batch. Case studies, including a "Red Team" Hold Flood attack simulation, demonstrate how dynamic evidence thresholds and Verifiable Delay Functions (VDFs) allow the system to "fail closed" under adversarial load, preserving systemic integrity.

Keywords: Anti-Money Laundering (AML), Ternary Logic, Distributed Ledger Technology (DLT), Merkle Trees, System Architecture, Epistemic Uncertainty, Verifiable Delay Functions (VDF), ISO 20022.

Infographic Presentention

I. Problem Statement: The Systemic Failure of Bivalent Compliance

The global Anti-Money Laundering (AML) regime is currently operating under a paradigm of systemic failure. Despite the proliferation of increasingly complex regulations and the expenditure of billions of dollars on compliance technology, the rate of illicit fund interdiction remains negligible, estimated by some observers to be below one percent of total criminal proceeds. To understand why AML fails, one must move beyond the traditional diagnosis of "poor data quality" or "insufficient staffing" and analyze AML as a fundamental failure of governance, evidence, and action-control logic. Current systems fail because they are built on a bivalent (binary) logic that is structurally incapable of managing economic action under epistemic uncertainty.

1.1 Structural Failures: The Interdiction Gap and Binary Model Brittleness

The primary structural flaw in modern AML architectures is the reliance on post-hoc reporting. The current standard of enforcement is the Suspicious Activity Report (SAR). In architectural terms, a SAR is a narrative document generated after an economic act has already been finalized. This creates what must be termed an "interdiction gap." By the time a compliance officer identifies a suspicious pattern and files a report with a Financial Intelligence Unit (FIU), the funds have typically moved through multiple jurisdictions and layered entities.1 Post-hoc reporting documents the failure of prevention; it does not provide a mechanism for real-time control.

Furthermore, the binary "Allow/Deny" switch that governs transaction processing is inherently brittle. In high-volume financial environments, liquidity is the paramount priority. Because a binary system offers only two terminal states—processing the transaction or killing it—any ambiguity or unresolved uncertainty is almost always absorbed into the "Allow" state to prevent liquidity friction.2 This "fail-open" bias means that the financial system essentially operates on a "trust-by-default" basis, where transactions proceed unless they hit a hard, pre-defined negative filter. This allows sophisticated adversaries to exploit the "blind spots" of binary filters by remaining just below threshold limits or utilizing emerging typologies that the system has not yet been programmed to "Deny".2

Operational failure modes are the natural consequence of this logical brittleness. Alert fatigue occurs because compliance teams are flooded with "false positives" that they must manually

resolve into "Yes" or "No" decisions under extreme pressure.5 Typology gaming and velocity exploitation occur because the system's logging is fragmented; the decision to allow a transaction is often separated from the evidence used to justify it. Silent overrides, where senior management or automated routines bypass compliance holds to satisfy a high-value client or a technical bottleneck, are rarely recorded with sufficient granularity for forensic audit.5

1.2 Liquidity vs. Integrity Modeling: The Economic Proof of Ternary Efficiency

A frequent objection to introducing more rigorous controls is that they introduce unacceptable friction. However, this objection relies on a flawed economic model that prices immediate velocity while ignoring long-term liability. Ternary Logic (TL) proposes a formal shift in how the economy of compliance is calculated, converting unbounded probabilistic risk into bounded, measurable latency.

The False Economy of Unverified Velocity

In the current bivalent model, the cost of a transaction $C_{tx}(A)$ is perceived as minimal because the latency is near zero. However, this ignores the downstream liability (L_{prob}) that remains attached to the institution for years. Because this liability is realized asynchronously—often during a regulatory audit or criminal investigation five to ten years after the fact—markets currently price it at zero. This leads to catastrophic repricing events, such as the multi-billion dollar fines seen in the correspondent banking sector over the last decade.
The liability equation is defined as:

$$L_{prob} = (P_{laundering} \times C_{fine}) + (P_{remediation} \times C_{audit}) + (P_{reputation} \times C_{market\_cap})$$
Where $P_{laundering}$ is the probability of a transaction being illicit, C_{fine} is the cost of the penalty, $P_{remediation}$ is the probability of a mandated audit, and C_{market_cap} represents the destruction of shareholder value.1 In a binary system, because uncertainty is pushed into the "Allow" state, L_{prob} remains unbounded and hidden until it is too late to mitigate.

The Ternary Logic Efficiency Model

The TL cost model replaces this hidden uncertainty with synchronous latency:

$$C_{tx}(TL) = C_{fee} + \Delta_{hold}$$
While Δ_{hold} (the latency of an Epistemic Hold) is non-zero, it drives L_{prob} toward zero by ensuring no transaction proceeds while uncertainty remains unresolved. Markets can efficiently price latency through Service Level Agreements (SLAs), derivatives, and liquidity management, but they cannot price retroactive uncertainty. Therefore, State 0 (the Hold) creates "higher-integrity liquidity" that protects the institution's balance sheet from future erasure.2

Variable	Current Binary Model	Ternary Logic Model
Latency	Near Zero	Bounded (Δ_{hold})
Evidence	Post-Hoc (SAR)	Pre-Action (Decision Log)
Risk Realization	Asynchronous / Delayed	Synchronous / Real-time
Tail Risk	Unbounded (L_{prob})	Bounded (Integrity-verified)
Market Pricing	Failure at tail-events	Efficient pricing of latency

II. Introducing Ternary Logic (TL): The Architecture of Doubt

Ternary Logic (TL) is a triadic action-governance architecture designed to govern economic acts based on evidence rather than intentions. It moves beyond the simplistic "Yes/No" paradigm to formalize the state of "I don't know" as a functional, mandatory governance gate.1

2.1 Defining the Triadic Action States

The core of TL resides in three distinct, mutually exclusive states of action:

1. **+1 Proceed (Action Permitted)**: The system possesses clear, verified evidence. The provenance of funds is established, the counterparty identity is verified, and the act conforms to all programmed mandates. The transition to State +1 is a deterministic outcome of satisfied evidence conditions.1
2. **0 Epistemic Hold (The Sacred Zero)**: This is the state of unresolved uncertainty. The system possesses insufficient evidence to Proceed (+1) but lacks the specific, verified cause required to Refuse (-1). The transaction is paused—not as a punishment, but as a mandatory evidentiary requirement. This state blocks the velocity of the transaction without presuming the guilt of the actor.1
3. **-1 Refuse (Action Denied)**: The system has identified a verified risk, a prohibited actor, or a clear violation of law. The harm is certain, and the refusal is logged as a deterministic outcome of policy violation.1

2.2 The Crucial Distinction: Risk in the Zero State

In the architecture of AML, risk does not reside in the "Deny" state; it resides primarily in the "Zero" state. Money laundering occurs when transactions characterized by high epistemic uncertainty—unknown owners, opaque origins, or anomalous patterns—are allowed to slide into the "+1 Proceed" state to maintain transaction volume. A system that allows a "0" to become a "+1" without the injection of additional, verifiable evidence is, by definition, a failed system. TL

ensures that State 0 is a hard logical barrier that requires the collapse of uncertainty before any economic action can manifest.2

III. Core TL Mechanisms for AML Enforcement

The implementation of TL requires a suite of technical mechanisms that ensure governance is native to the execution of the transaction itself, rather than an external oversight layer.

3.1 Epistemic Hold: Blocking Velocity without Presumption

The Epistemic Hold is triggered by specific, programmable evidentiary gaps, such as incomplete provenance data, counterparty opacity, jurisdictional risk (e.g., conflict zones), or structural anomalies in transaction volume. Unlike a "freeze" in the traditional sense, which often requires a manual legal order, the Hold is an automated, runtime requirement of the logic itself. It effectively "halts" the laundering process by stopping the movement of value until the necessary data is provided to resolve the uncertainty.1

3.2 Decision Logs: "No Log = No Action"

The foundational rule of TL is "No Log = No Action." This means that the system is physically and logically incapable of executing an economic transaction—such as a wire transfer or a credit disbursement—until a Decision Log has been initiated and signed. These logs are not summaries; they are pre-action records that capture three critical dimensions of the moment of decision:

- **What was known**: The specific inputs and verified data points available.
- **What was unknown**: The specific missing variables or evidence gaps.
- **What was assumed**: The risk thresholds and heuristic rules applied to bridge the gap between uncertainty and action.2

3.3 Immutable Ledger and the Hybrid Shield

All Decision Logs are recorded on a tamper-evident, immutable ledger. To maintain the necessary separation between transaction performance and compliance integrity, TL utilizes a Hybrid Shield architecture. This prevents silent overrides by ensuring that any deviation from the system's recommended state (e.g., a human forcing a +1 state on a 0-state transaction) is recorded immutably. The shield captures the identity of the person performing the override, the timestamp, the specific authority they invoked, and their provided rationale. This ensures that "God Mode" access, a common vulnerability in traditional banking databases, is eliminated.2

3.4 Anchors: Evidentiary Permanence via Merkle Roots

Long-term evidentiary permanence is achieved through anchoring. Every Decision Log is hashed and grouped into batches, with the Merkle root of the batch anchored to one or more

external, public blockchains or trusted time-stamping services. This anchoring process ensures that the records cannot be deleted or "revised" following a regulatory scandal. It provides a mathematical proof of the system's state at a specific point in history.2

3.5 The AI-to-Logic Handoff: Governance of Probability

Modern AML often relies on Machine Learning (ML) models that produce probabilistic risk scores (e.g., "Risk: 0.72"). In a binary system, these scores are often misinterpreted as authorization. TL treats these scores as indicators of epistemic uncertainty.
The logic for the handoff is as follows:

- **If Score < Threshold_Low**: The uncertainty is low; move to State +1.
- **If Score > Threshold_High**: The risk of harm is high; move to State -1.
- **If Threshold_Low < Score < Threshold_High**: The system acknowledges genuine ambiguity; move to State 0 (Epistemic Hold).

No transaction proceeds until the uncertainty represented by the 0.72 score collapses into a deterministic +1 or -1 through the acquisition of more evidence. This prevents the "normalization of deviance" where high-risk transactions are routinely processed because they don't quite hit a "Deny" threshold.3

IV. Technical Architecture for AML at Scale

Scaling TL to handle the millions of transactions per second required by global payment networks necessitates a dual-lane latency architecture and sophisticated cryptographic batching.

4.1 Dual-Lane Latency Architecture: Solving the Friction Tension

To resolve the tension between sub-millisecond settlement speeds and the requirement for robust evidence, TL employs a bifurcated processing model.9

Feature	**Fast Lane**	**Slow Lane (Asynchronous)**
Target Latency	≤ 2ms	≤ 500ms
Primary Task	State Check (+1, 0, -1)	Log Enrichment & Sealing
Integrity Check	Query Current Decision State	Cryptographic Sealing
Logging	Initiate Log Header	Finalize & Anchor Log
Outcome	Immediate Economic Action	Long-term Proof Generation

The Fast Lane initiates the Decision Log header (capturing Context ID and Intent Hash), ensuring that no economic action occurs before a record is started. The Slow Lane completes the enrichment and anchoring in parallel, ensuring that the "compliance passport" is finalized without delaying the transaction flow.4

4.2 Merkle-Batched Anchoring: Achieving O(1) Scalability

Anchoring every individual transaction log would be prohibitively slow ($O(n)$). TL utilizes Merkle Batching to achieve constant-time scalability ($O(1)$) per batch. Individual logs are hashed and structured into Merkle Trees; only the 32-byte Merkle root is anchored to an external ledger. This allows for $O(\log_2 n)$ verification, where an auditor can verify any single record's integrity within a batch of millions using only a handful of hashes.8 This is a structural requirement for any system intended to function as a global settlement layer.

4.3 Deferred Anchoring and Compliance Debt

In ultra-high-performance environments like High-Frequency Trading (HFT), TL allows for "Deferred Anchoring." In this mode, evidence is generated in real-time, but anchoring to public ledgers is time-bounded (e.g., every 60 seconds). Failure to anchor within the defined window is treated as a severe compliance violation—essentially "compliance debt" that must be settled before the system can return to a healthy state. If the debt remains unpaid, the system is programmed to "fail closed" to State -1 for all new transactions.2

4.4 Privacy, GDPR, and Ephemeral Key Rotation (EKR)

TL addresses the "Right to Erasure" (GDPR) by pseudonymizing data before hashing. When a user requests the deletion of their data, the off-chain log can be removed, but the on-chain hash remains as a "shredded" proof of the transaction's historical integrity. Furthermore, Ephemeral Key Rotation (EKR) is used to grant auditors time-limited access keys that automatically expire, ensuring that trade secrets and sensitive financial data are protected from unauthorized long-term exposure.2

4.5 ISO 20022 Semantic Mapping: Interoperability

Interoperability with the existing financial ecosystem is achieved by mapping TL states to ISO 20022 pacs.002 (Payment Status Report) codes.14

Ternary State	**ISO 20022 Status Code**	**Mapping Logic**
+1 Proceed	**ACCP** (Accepted)	Evidence is verified; funds move.
0 Epistemic Hold	**PDNG** (Pending)	Held for manual/system verification.

Ternary State	ISO 20022 Status Code	Mapping Logic
-1 Refuse	**RJCT** (Rejected)	Prohibited actor/harm detected.

The Decision Log hash is injected into the SupplementaryData field of the ISO message. This ensures that the "compliance proof" travels with the transaction, allowing the receiving bank to verify that the sending bank has already resolved the epistemic uncertainty.14

V. Regulatory, Legal, and Operational Alignment

Ternary Logic is designed to operationalize existing regulatory mandates into hard technical controls, shifting compliance from a "best effort" policy to a "runtime requirement."

5.1 Regulatory Alignment: Operationalizing Global Frameworks

TL provides the technical bridge for frameworks like the FATF Travel Rule, which requires the exchange of originator and beneficiary information. Under TL, a transaction with missing Travel Rule data is automatically placed in State 0. The transaction cannot move until the counterparty provides the signed data packet required to collapse the state into +1.1 This transforms the Travel Rule from a reporting burden into an automated gate for liquidity. Similarly, TL helps banks meet the "operational risk" requirements of Basel III by providing a real-time monitor of the "integrity health" of the transaction pool.2

5.2 Comparative Operational Analysis

The following tables evaluate TL against current industry standards across multiple domains of governance and risk management.

Table 1: Risk and Capital Management (Basel III vs. TL)

Metric	Basel III Approach	Ternary Logic Approach
Control Mechanism	Capital buffers (Ex-post)	Runtime state constraints (In-situ)
Operational Risk	Statistical modeling of loss events	Logical prevention of unverified acts
Liquidity Treatment	Assumes liquidity is binary	Differentiates between verified and unverified liquidity

Metric	Basel III Approach	Ternary Logic Approach
Stress Testing	Focuses on capital adequacy	Focuses on evidence-to-action ratios

Table 2: Market Integrity (IOSCO Principles vs. TL)

Metric	IOSCO Principles	Ternary Logic Implementation
Surveillance	Post-trade anomaly detection 17	Pre-trade evidence verification 2
Transparency	Disclosure of intent and identity	Cryptographic proof of identity and provenance
Market Abuse	Detect and prosecute after the fact	Prevent through State 0 holds on ambiguous trades
Reporting	Periodic regulatory filings	Continuous, real-time anchored logs 3

Table 3: Record Keeping and Security (SEC/CFTC & NIST vs. TL)

Metric	SEC/CFTC WORM Storage	NIST Pause/Verify	Ternary Logic (TL)
Data Integrity	Write Once, Read Many (Static)	Identity/Credential Verification 20	Multi-chain Anchored Hashing (Active)
Access Control	Permissions-based	Zero Trust Architectures 20	Hybrid Shield & EKR 2
Evidence Chain	Sequential log files	Audit trails	Merkle-Tree Chain of Custody 8
Response	Investigative	"Human Firewall" 20	Automated State 0 Hold

Table 4: Audit Standards (SOX/COSO vs. TL)

Metric	SOX/COSO Standard	Ternary Logic (TL)
Verification	Statistical sampling of transactions 22	100% cryptographic verification of all acts
Control Environment	Management attestation of policies	Code-level enforcement of logic 3
Evidence Quality	Paper/Digital trails with human signatures	Multi-signed, anchored, immutable proofs
Timeliness	Annual/Quarterly audit cycles	Continuous, real-time "Proof of Logic"

VI. Evidence, Liability, and Enforcement

The transition to TL fundamentally alters the enforcement posture of regulators and the liability profile of financial institutions.

6.1 Reverse Burden of Proof: "The Missing Log"

In the current regime, a regulator must prove that an institution acted with "willful blindness" or "knowledge" of money laundering. In a TL-governed system, the burden of proof shifts. Because the architecture mandates "No Log = No Action," the absence of a Decision Log for a processed transaction is prima facie evidence of gross negligence.2 If a transaction proceeded from State 0 to State +1, the bank must defend the specific rationale captured in the Decision Log. This makes the compliance officer's reasoning a matter of forensic record, not a post-hoc memory.5

6.2 Admissibility and the Chain of Custody

The completeness of TL logs makes them highly admissible as digital evidence in criminal prosecutions. Merkle proofs establish a mathematical "Chain of Custody" (CoC) that proves exactly when a decision was made and that the record has not been tampered with since its creation.8 This simplifies the work of courts and investigators, moving the legal focus from "What did they know?" to "Why did they act on this specific evidence?".11

VII. Case Studies: Simulating TL in AML Scenarios

The following scenarios demonstrate how TL resolves common AML failure points in high-risk transaction chains.

7.1 Cross-Border Correspondent Banking: Resolving UBO Opacity

The Problem: A bank in a "grey-list" jurisdiction sends a $50 million wire to a major global hub. The Ultimate Beneficial Owner (UBO) is a shell company in the British Virgin Islands. **The Simulation**: The system triggers **State 0 (Epistemic Hold)** due to "UBO Opacity." The funds are held at the gateway. The "Hold Room" interface automatically requests the sending bank to provide a signed proof of UBO. The sending bank provides a cryptographically signed identity packet. The TL system verifies the packet against a trusted UBO registry. The state collapses to **+1 (Proceed)**, and the funds settle in 15 seconds. **Insight**: Liquidity was delayed by seconds, but the risk of processing an illicit transaction was reduced to near zero. The decision and the UBO evidence are anchored immutably.5

7.2 Shell-Company Transaction Chain: Detecting Layering

The Problem: A network of entities performs 200 transfers of $9,500 each to avoid the $10,000 reporting threshold (structuring). **The Simulation**: While individual transactions might pass low-level filters, the TL "Aggregate Context" engine detects the pattern and triggers a **Sacred Pause (State 0)** on the 10th transaction in the sequence. A Decision Log is created documenting the "Structuring Pattern." The system requires a human compliance officer to review the cluster. The officer identifies the layering and shifts the cluster to **State -1 (Refusal)**. **Insight**: The system "failed closed" to protect the integrity of the network rather than allowing the Structuring attempt to succeed.3

7.3 Crypto-Fiat Laundering Bridge: Proof of Wallet at the Off-Ramp

The Problem: An entity attempts to convert $10 million in BTC to USD at a fiat bank. The BTC history shows a recent interaction with a sanctioned mixer. **The Simulation**: The bank's TL interface triggers **State 0** because the "Provenance Chain" is broken by the mixer. The system requires "Proof of Non-Sanctioned Source." The user fails to provide the proof. The system moves to **State -1** and notifies the relevant FIU, anchoring the refusal log as evidence. **Insight**: TL prevents the "fiat exit" by enforcing evidence requirements at the bridge.3

7.4 Red Team Scenario: The Hold Flood Attack

The Problem: An adversary attempts to paralyze a bank by flooding it with millions of ambiguous transactions, all designed to trigger State 0 and overwhelm the compliance team. **The Simulation**: The TL system detects the spike in State 0 volume. It triggers "Dynamic Evidence Thresholds." The cost to enter State 0 increases (the system requires more certainty

to *hold* than to *refuse*). Ambiguous transactions that previously triggered State 0 are now automatically shifted to **State -1 (Refuse)**. **Insight**: The system maintains its integrity by failing to a "Refuse" state under attack, ensuring that the adversary cannot "DDoS" their way through the compliance gate.2

VIII. Strategic Recommendations

To achieve the global adoption of Ternary Logic, the following actions are recommended:

1. **For Regulators (FATF, Central Banks)**: Mandate "Proof of Logic" for all high-volume settlement systems. Require that no economic action can occur without a corresponding anchored Decision Log.
2. **For Banks**: Transition to a dual-lane architecture. Decouple transaction settlement from evidence anchoring while maintaining the "No Log = No Action" constraint.
3. **For Payment Networks**: Update ISO 20022 implementation guides to require the injection of Decision Log hashes in the pacs.002 supplementary data fields.
4. **For Auditors**: Shift from annual sampling to real-time, 100% verification of anchored Merkle roots.

IX. Foundational Origin Note

The structural and ethical foundations of Ternary Logic are rooted in a specific triadic commitment to truth and action.
“The Goukassian Vow was articulated by Lev Goukassian during a period of terminal lucidity associated with his stage-4 cancer diagnosis. This moment of absolute clarity produced the triadic ethic that underpins TL’s mechanism.” 7

The Goukassian Vow:

- **Pause when truth is uncertain.**
- **Refuse when harm is clear.**
- **Proceed where truth is.** 5

In the context of AML, this vow manifests as the "Sacred Zero"—the mandatory hesitation that ensures the financial system never mistakes the speed of liquidity for the presence of truth. By hard-coding this ethic into the logic of global finance, we move from a system of "trusted intent" to a system of "verified action," finally closing the interdiction gap that has plagued AML for decades.2

Works cited

1. FractonicMind/TernaryLogic: Ternary Logic enforces ... - GitHub, accessed February 9, 2026, https://github.com/FractonicMind/TernaryLogic

2. The Day the House Entered Epistemic Hold: A Story of Ternary ..., accessed February 9, 2026, https://hackernoon.com/the-day-the-house-entered-epistemic-hold-a-story-of-ternary-logic-congress-and-credible-evidence
3. LOGIC IS CONSTITUTION: WHY MACHINES NEED PERMISSION TO SAY "I DON'T KNOW" | by Lev Goukassian - Medium, accessed February 9, 2026, https://medium.com/@leogouk/logic-is-constitution-why-machines-need-permission-to-say-i-dont-know-d3611100615b
4. How an Email from a Stranger Saved My Sanity (and Maybe AI) | by Lev Goukassian, accessed February 9, 2026, https://medium.com/@leogouk/how-an-email-from-a-stranger-saved-my-sanity-and-maybe-ai-2c282e163041
5. Date Night at the Sacred Zero. When a quiet Saturday dinner… | by ..., accessed February 9, 2026, https://medium.com/@leogouk/date-night-at-the-sacred-zero-e3764663708c
6. The UNESCO Bluff: Giving the World's AI Principles Guts | by Lev Goukassian - Medium, accessed February 9, 2026, https://medium.com/@leogouk/the-unesco-bluff-giving-the-worlds-ai-principles-guts-f5d5896526dd
7. Good News: You Don't Need to Rewrite the Standard | by Lev Goukassian - Medium, accessed February 9, 2026, https://medium.com/@leogouk/good-news-you-dont-need-to-rewrite-the-standard-2ff9afdc2282
8. BLOCKCHAIN FOR LEGAL EVIDENCE MANAGEMENT: ENHANCING TRANSPARENCY AND SECURITY IN JUDICIAL SYSTEMS - International Journal of Environmental Sciences, accessed February 9, 2026, http://theaspd.com/index.php/ijes/article/download/419/361/1426
9. Six Tech CEOs Accidentally Read the Wrong Paper and Nearly, accessed February 9, 2026, https://medium.com/@leogouk/six-tech-ceos-accidentally-read-the-wrong-paper-and-nearly-rewrote-reality-84d21a856481
10. ESTABLISHING A LEGALLY DEFENSIBLE BLOCKCHAIN CHAIN OF CUSTODY TECHNICAL FRAMEWORK - Scholars' Bank, accessed February 9, 2026, https://scholarsbank.uoregon.edu/bitstreams/6a3d005b-957e-4f9b-bbbb-a6589d9b798d/download
11. A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques - Preprints.org, accessed February 9, 2026, https://www.preprints.org/manuscript/202403.0703
12. Qubic AI technology page - Lablab.ai, accessed February 9, 2026, https://lablab.ai/tech/qubic
13. VeraSnap and the IETF: One Developer's Quest to Make Digital Evidence Trustworthy in the Age of AI - DEV Community, accessed February 9, 2026,

https://dev.to/veritaschain/verasnap-and-the-ietf-one-developers-quest-to-make-digital-evidence-trustworthy-in-the-age-of-ai-1bad
14. A DEEP DIVE ON PACS.004 & 002 - BNY, accessed February 9, 2026, https://www.bny.com/assets/corporate/documents/pdf/iso-20022/learning-guide-module-6.pdf
15. ISO 20022 Messages Overview - FedNow Service, accessed February 9, 2026, https://explore.fednow.org/resources/readiness-guide-iso-20022.pdf
16. pacs.002 ISO 20022 message: FI To FI Payment Status Report, accessed February 9, 2026, https://www.cpg.de/en/glossary/pacs-002-iso-20022-message/
17. Ireland: Detailed Assessment of Observance of IOSCO Objectives and Principles of Securities Regulation; IMF Country Report 14/13, accessed February 9, 2026, https://www.centralbank.ie/docs/default-source/tns/about---tns/peer-reviews-and-reports/tns-1-11-imf-report-on-observance-of-standards-and-codes-on-securities-regulation.pdf
18. ASIC's priorities for the supervision of market intermediaries, accessed February 9, 2026, https://www.asic.gov.au/regulatory-resources/markets/market-supervision/asic-s-priorities-for-the-supervision-of-market-intermediaries/
19. Financial Markets Review final report 2020 - South African Reserve Bank, accessed February 9, 2026, https://www.resbank.co.za/content/dam/sarb/publications/media-releases/ad-hoc-news/2020/9751/Financial-Markets-Review-final-report-2020.pdf
20. Skeptical By Design - Stop Trusting and Start Verifying - Morefield, accessed February 9, 2026, https://morefield.com/blog/skeptical-by-design-stop-trusting-and-start-verifying/
21. Social Engineering Attacks: Cybercriminal Tactics & Psychology - TechBrain, accessed February 9, 2026, https://www.techbrain.com.au/social-engineering-attack-psychology/
22. IoT-Enabled Tokenization of Physical Assets - SEC.gov, accessed February 9, 2026, https://www.sec.gov/files/ctf-written-input-daniel-bruno-corvelo-costa-092125.pdf
23. Blockchain Based Framework for Securing Digital Evidence - SciTePress, accessed February 9, 2026, https://www.scitepress.org/Papers/2025/138853/138853.pdf
24. The Day the SEC Stopped Lying to Itself | by Lev Goukassian | Medium, accessed February 9, 2026, https://medium.com/@leogouk/the-day-the-sec-stopped-lying-to-itself-6559c353b67d
25. Six People, One Binder, and No Way Back. | by Lev Goukassian - Medium, accessed February 9, 2026, https://medium.com/@leogouk/six-people-one-binder-and-no-way-back-f812fabd00f1