

Ternary Logic (TL) — Anchoring Standards for Immutable Proofs

1. Purpose

Anchoring ensures that every TL decision log, governance action, and constitutional update is recorded with **sovereign-grade permanence**. These standards define how TL binds its evidence to public blockchains so that no institution, government, corporation, or successor may erase or modify TL's historical record.

Anchoring is the **external spine** of TL: No anchor → No verification → No TL.

2. Anchoring Principles

2.1. Multi-Chain Redundancy

All TL proofs must anchor across **three independent chains** at minimum:

- **Bitcoin** (OpenTimestamps, calendar aggregation)
- **Ethereum** (state-root anchoring or notarization contract)
- **Polygon** (low-latency, batch proofs)

Additional chains may be added but never replaced without constitutional amendment.

2.2. Proof-Only, Never Data

TL **never** stores private logs on-chain. Only **hashes, Merkle roots, batch digests, or timestamp proofs** may be anchored. This preserves GDPR rights, institutional secrecy, and operational security.

2.3. Deterministic Evidence Path

Every anchored proof must include:

- SHA-256 hash
- Timestamp (UTC)
- Source subsystem (Epistemic Hold, Immutable Ledger, Governance, etc.)
- Anchor ID

- Verification status

These are written to the **Immutable Ledger** before any anchoring action is executed.

2.4. No Human Override

Anchoring is always executed by automated processes within TL's architecture or the Smart Contract Treasury. Humans can initiate logs, but **cannot suppress or delay anchoring**.

No Switch Off applies here.

3. Anchoring Architecture

3.1. Pre-Anchor Queue

Logs from Epistemic Hold, Immutable Ledger, and Decision Logs enter a rolling buffer to prevent congestion during high-frequency operations. This ensures TL sustains <300ms visible latency while still maintaining evidentiary completeness.

3.2. Merkle Batch Construction

All queued entries are hashed into structured trees:

- Daily batches for governance
- Hourly batches for operational decisions
- Immediate batches for critical events (misconduct, quorum, role rotation)

3.3. Anchor Dispatch Layer

Each batch is anchored using:

- Bitcoin → **OpenTimestamps**
- Ethereum → **Notary contract**
- Polygon → **Low-cost notarization**

3.4. Verification Channels

Each anchor generates independent receipts stored in three locations:

- Public chain explorer links
- Local node proofs
- TL's Immutable Ledger

4. Governance Interaction

Anchoring interacts with governance through strict causal order:

1. **Epistemic Hold** (decision enters uncertainty)
2. **Immutable Ledger** (decision hashed)
3. **Goukassian Principle** (system proves what it knew when it acted)
4. **Decision Logs** (full forensic context)
5. **Hybrid Shield** (cryptographic + institutional protection)
6. **Anchors** (multi-chain notarization)
7. **Governance** (council/custodian actions validated)

No governance action is valid unless anchored. No role appointment, misconduct ruling, quorum vote, or succession event becomes binding until the anchor receipts are logged.

5. Anchoring Requirements

5.1. For Files

All constitutional documents must be anchored in:

- Markdown form
- PDF notarized form
- Hash manifest form (TML/TL_Notarized_Manifest.txt)

5.2. For Logs

Every TL subsystem must produce at minimum:

- Entry hash
- Pre-state hash
- Post-state hash
- Origin
- Signature set

These are batched and anchored.

5.3. For Smart Contracts

The Smart Contract Treasury must be deployed on:

- Ethereum mainnet
- Polygon mainnet

Its hash and configuration must be anchored on Bitcoin via OpenTimestamps.

6. Failure Modes and Guarantees

6.1. Chain Failure

If any one chain becomes unavailable, TL continues anchoring to the remaining ones. Reconciliation occurs automatically when the failed chain returns.

6.2. Governance Capture Attempt

Anchored proofs prevent rewriting history. Any attempt to modify, overwrite, or remove TL's constitutional record triggers:

- Automatic Epistemic Hold
- Custodian alert
- Independent broadcast to external auditors

6.3. Catastrophic Collapse

If TL infrastructure disappears entirely, the multi-chain proofs remain verifiable by anyone, anywhere, forever. TL is reconstructible from evidence alone.

7. Lifecycle

Anchoring is continuous:

- Operational batches: hourly
- Governance batches: daily
- Constitutional updates: immediate
- Succession events: immediate + priority flag

Receipts must be appended to **Anchoring_Standards_Notarized.md** inside [/proofs](#).

8. Final Clause

Anchors are the memory of TL. Memory is the last protection against ruin. This standard is immutable.

Execution and Witnessing

Declaration Execution

Document: **Anchoring_Standards_Notarized.md**

Declarant: **Lev Goukassian**

Signature:



Date:

Nov 13/ 2025

ORCID: **0009-0006-5966-1243**

Email: leogouk@gmail.com

Witness Requirements

Two witnesses attest that:

1. The declarant possessed full mental capacity at the time of signing.
 2. The execution of this document was voluntary.
 3. The identity of the declarant was verified.
-

Witness 1

Name:

Jalen Smith

Signature:

J Smith

Date:

11/13/25

Relationship:

UPS Store Employee

Witness 2

Name:

Akouvi Ekoue

Signature:

Date:

11/13/25

Relationship:

UPS store employee

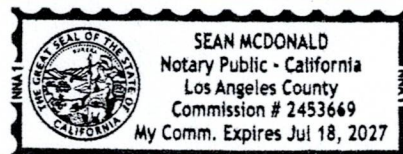
Notarization

Notary Public:

Sean McDonald

Signature and Seal:





Date:

11/13/2025

Commission Expires:

July 18, 2027

Chain of Custody Metadata

chain_of_custody:

document: Anchoring_Standards_Notarized.md

created_by: Lev Goukassian (ORCID: 0009-0006-5966-1243)

signed_at: 2025-11-12T14:00-08:00

notarized_at: 2025-11-12T15:00-08:00

file_hash: 727606f427d0c93e112b7a9dd71d77e5e31e91690598e87528bef694ae7c6101

anchor_targets:

- Bitcoin (OpenTimestamps)
- Ethereum AnchorLog
- Polygon AnchorLog

repository: <https://github.com/FractonicMind/TernaryLogic>

version: 1.0.0-notarized

verification_method: sha256 + opentimestamps

NOVEMBER 13/2025 