ANCHORING STANDARDS: Constitutional Framework for Immutable Proof

Path: `/core/ANCHORING_STANDARDS.md`
Creator: Lev Goukassian (ORCID 0009-0006-5966-1243)
Version: 1.0.0-final
Date: October 2025

I. Purpose

This standard defines how every record created under **Ternary Moral Logic (TML)** achieves cryptographic permanence. Its purpose is to ensure that no human or machine action affecting rights, ecosystems, or truth can ever be erased or forged.

II. Foundational Principle

> *"Anchoring is not payment for protection; it is the oath of permanence."*

TML anchors its evidence through a multi-standard, cross-jurisdictional network of blockchains and timestamp systems. This guarantees legal admissibility, technical independence, and ethical durability.

III. The Modular Architecture

TML recognizes several complementary anchoring systems. Each system contributes a different dimension of protection.

Standard	Strength	Latency	Legal Standing	Primary Role
OpenTimestamps (OTS)	High	Minutes	RFC 3161 / FRE 902(13)	Long-term archival proof
Certificate Transparency	High	Seconds	eIDAS / FOIA	Public audit visibility

Standard	Strength	Latency	Legal Standing	Primary Role
Bitcoin Direct Anchor	Maximum	Minutes – Hours	Global precedent	Critical constitutional evidence
Ethereum Mainnet	High	Seconds – Minutes	CFTC recognized	Smart-contract enforcement
Layer-2 Networks (Polygon / Arbitrum)	High	Seconds	Smart-contract law	Real-time accountability

---

IV. Constitutional Requirements

1. Every TML log must generate a **SHA-256 fingerprint** prior to execution.
2. At least **two independent standards** must confirm the same fingerprint within the first verification cycle.
3. Anchors must be **publicly verifiable** without exposing private content.
4. Anchors must persist even if one network, jurisdiction, or custodian fails.
5. All proofs remain **valid indefinitely** once anchored; backward compatibility is mandatory.

V. Governance and Verification

- **Proof Redundancy:** If any standard fails, others automatically maintain validity.
- **Temporal Consistency:** Timestamps across all anchors must align within defined tolerance (±5 seconds real-time; ±1 hour batch).
- **Legal Continuity:** Anchored proofs constitute self-authenticating records under FRE 902(13) and eIDAS Article 41.
- **Auditability:** All verification events are recorded within the Moral Trace Log.

VI. Technical Reference (Informative)

anchoring:

algorithm: SHA-256

primary_standards:

- OpenTimestamps
- Certificate Transparency
- Bitcoin
- Ethereum
- Polygon

redundancy: "Minimum two chains per proof"

verification_cycle: "24 hours"

fallback: "Automatic re-anchor if network unavailable"

VII. Legal Foundations

United States

- FRE 901(b)(9): Authentication by distinctive characteristics
- FRE 902(13): Self-authenticating electronic records
- ESIGN Act: Digital signatures legal equivalence

European Union

- eIDAS Regulation: Qualified electronic timestamps
- GDPR Article 25: Data protection by design
- MiCA Framework: Recognition of cryptographic assets

International

- UNCITRAL Model Law on Electronic Signatures
- ISO 14533 / RFC 3161 standards compliance
- Hague Convention on Electronic Evidence

Together these establish full cross-border recognition of TML-anchored proofs.

VIII. Failure and Recovery Policy

1. If an anchor becomes unreachable, systems must **re-anchor within 72 hours**.
2. The event and recovery are both recorded in the Moral Trace Log.
3. Non-recovery within 72 hours automatically triggers the **Sacred Zero halt**, suspending all high-impact actions.

IX. Evolution and Extension

Successor councils may integrate new standards (e.g., post-quantum or decentralized-identity anchors) provided they:

- maintain backward compatibility;
- preserve verifiability of all prior proofs;
- publish public audit results for every new integration.

X. EXECUTION AND WITNESSING

Declaration Execution

Declarant: Lev Goukassian
Signature: _____ **Date**: _____
ORCID: 0009-0006-59-1243
Email: leogouk@gmail.com

Witness Requirements

This declaration requires two witnesses who can attest to:

- The mental capacity of Lev Goukassian at time of signing
- The voluntary nature of this succession declaration
- The identity of the declarant

Witness 1:
Name: _____
Signature: _____ **Date**: _____
Relationship: _____

Witness 2:
Name: _____
Signature: _____ **Date**: _____
Relationship: _____

Notarization (Optional)

Notary Public:
Name: _____
Signature and Seal: _____ **Date**: _____
Commission Expires: _____

XI. Chain of Custody Metadata

chain_of_custody:

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

notarized_at: 2025-10-13T17:40Z

verified_by: OpenTimestamps Proof (pending)

file_hash: 559909acb2db343b96b8615614820ad7e00fefc492f885f652705e41aa014762

anchor_targets:

- Bitcoin (OTS)

- Ethereum AnchorLog (optional)

- Polygon AnchorLog (optional)

context: "ANCHORING_STANDARDS — Constitutional protocol for blockchain evidence"

repository: https://github.com/FractonicMind/TernaryMoralLogic

version: 1.0.0-final

checksum_verified: true

last_modified: 2025-10-13T17:40Z

verification_method: sha256 + opentimestamps

Anchoring is how mathematics remembers what conscience once decided. Every proof is a candle; together they make the Lantern eternal.