Evidence Architecture

Cryptographic governance infrastructure for institutional accountability

Evidence Graph (EDG) Overview

ETHRAEON's core innovation is the **Evidence Directed Graph (EDG)**—a cryptographic structure where every governance action generates an immutable evidence node. Unlike blockchain (designed for trustless consensus), EDG is designed for *institutional accountability*: proving that authorized actions happened as documented, without requiring decentralized validation.

Evidence Node Structure

Core Components

- **Content Hash:** SHA-256 hash of action data (who, what, when, where)
- **Timestamp:** Cryptographically signed Unix timestamp (prevents backdating)
- **Authority Signature:** Digital signature of authorized actor (ministry, official, system)
- **Parent Nodes:** Links to previous related evidence (chain-of-custody)
- **Metadata:** Action type, constitutional tier (T0-T5), audit tags

Example Evidence Node (Humanitarian Aid)

```
{
  "node_id": "EDG-HA-20260104-00234",
  "content_hash": "a7f3c8d9e2b1...",
  "timestamp": "2026-01-04T14:23:17Z",
  "action": "Aid Border Entry",
  "authority": "Ukrainian State Customs Service",
  "data": {
    "aid_package_id": "WFP-2026-1543",
    "contents": "5 tonnes medical supplies",
    "entry_point": "Lviv Border Crossing"
  },
  "parent_nodes": ["EDG-HA-20260103-00198"],
  "constitutional_tier": "T3"
}
```

Constitutional Tiers (T0-T5)

Evidence nodes are classified by **rigidity level**, defining immutability and enforcement:

- **T0 (Suggestions):** Advisory recommendations, no enforcement
- **T1 (Best Practices):** Encouraged patterns, warnings if violated
- **T2 (Standard Patterns):** Expected norms, logged if deviated
- **T3 (System Constraints):** Required for operation, violations block execution
- **T4 (Security/Legal):** Mandatory compliance, violations trigger alerts + audits
- **T5 (Constitutional Law):** Immutable rules, violations halt system pending review

Tamper-Evidence Mechanisms

1. Immutability

Evidence nodes are **append-only**. Deletions are impossible; corrections generate new

nodes referencing the original (preserving error history).

2. Chain-of-Custody

Each node links to parent nodes, creating verifiable chains. Breaking a link (e.g., missing Node #42 in chain of 50) is instantly detectable.

3. Cryptographic Signing

Authorized actors digitally sign evidence nodes. Any modification invalidates signature, proving tampering.

4. Timestamp Integrity

Timestamps are signed by trusted time sources (NTP servers, government time authority). Backdating attempts create hash mismatches.

5. Distributed Replication

Critical evidence nodes replicated across multiple custody holders (government archives, donor servers, international observers). Tampering requires compromising all copies simultaneously.

Integration with Existing Systems

ETHRAEON does NOT replace operational systems. It sits beneath them as the governance layer:

Operational System → ETHRAEON Pattern

1. User performs action in existing system (e.g., customs officer logs aid entry)
2. System calls ETHRAEON API to emit evidence node
3. ETHRAEON validates action (authority check, constitutional compliance)
4. If valid, evidence node created + hash returned to operational system

5. Operational system stores hash alongside action record
6. Future audits verify: hash in operational system matches ETHRAEON evidence chain

Audit & Verification

Ministry Dashboards

Authorized officials access real-time evidence chains via web dashboards:

- View all evidence nodes for specific project, transaction, or entity
- Verify chain completeness (no missing nodes)
- Check authority signatures (who authorized each action)
- Export evidence bundles for external audits

Donor Portals

International donors receive custom views:

- Track funds from commitment → project completion
- Verify compliance with donor conditions (e.g., "funds used only for infrastructure")
- Download audit-ready evidence packages (quarterly/annual reporting)

Public Transparency

Select evidence nodes (non-sensitive) made publicly viewable:

- Citizens verify reconstruction project progress
- Civil society monitors aid distribution
- Journalists investigate discrepancies

Privacy & Confidentiality

Evidence integrity does NOT require public visibility:

- **Sensitive Data:** Encrypted in evidence nodes, decryptable only by authorized parties
- **Anonymized Reporting:** Whistleblower identities hashed (protected unless court order)
- **Tiered Access:** Different stakeholders see different evidence levels (citizen vs. auditor vs. prosecutor)
- **Judicial Seals:** Courts can temporarily seal evidence during active investigations

Evidence Persistence

Storage Duration: Evidence nodes stored indefinitely (no expiration). Critical for:

- Long-term project audits (reconstruction projects lasting 5-10 years)
- War crimes investigations (evidence may be used years after events)
- Institutional memory (proving past decisions for future policy)

Archival Strategy:

- Active nodes (last 2 years): Hot storage, real-time access
- Historical nodes (2-10 years): Warm storage, retrieval within 24hrs
- Archive nodes (10+ years): Cold storage, retrieval within 7 days

Compliance Standards

- **NIST Cybersecurity Framework:** Evidence integrity aligns with NIST CSF Identify/Protect functions
- **ISO 27001:** Information security management (cryptographic controls)
- **GDPR:** Personal data protection (encryption, access controls, right to explanation)

- **WCAG 2.1 Level AA:** Accessibility for dashboards and public portals
- **EU eIDAS:** Electronic signatures and trust services (for authority verification)
