Elara Core Whitepaper v2.0.0

Universal Data Integrity via the Directed Acyclic Mesh Protocol

Author: Nenad Vasic **Date:** February 2026 **Status:** Draft **Patent:** US Provisional 63/983,064 (Priority: February 14, 2026) **License:** BSL-1.1

Abstract

The Directed Acyclic Mesh (DAM) protocol provides a universal foundation for data integrity across domains ranging from healthcare to defense. This paper presents the Elara system — a lean implementation (~3,000 lines) that applies one cryptographic protocol to seven distinct domains through a thin adapter pattern. Each domain adapter defines record schemas, classification rules, compliance requirements, and threat models while sharing a common protocol layer featuring post-quantum dual signatures (Dilithium3 + SPHINCS+), hash-chained continuity, and causal DAG storage.

1. Problem Statement

Data integrity failures cost billions annually across every sector:

- **Medical:** ~250,000 deaths/year from medical errors (Johns Hopkins). Tampered records, broken audit trails, and unauthorized access to PHI remain systemic.
- **Industrial:** Supply chain fraud exceeds $40B annually. Sensor data without cryptographic provenance enables quality falsification.
- **AI Systems:** Large language models exhibit amnesia between sessions. No verifiable chain of cognitive continuity exists.
- **Education:** Academic fraud affects 1 in 6 researchers. Credential forgery undermines institutional trust.
- **Finance:** Regulatory non-compliance results in $10B+ in annual fines. Transaction records lack cryptographic immutability.
- **Defense:** Classified data chains require post-quantum resistance as quantum computing advances.
- **Agriculture:** Food safety recalls cost $10B annually. Farm-to-table provenance remains largely paper-based.

The common thread: **data lacks verifiable provenance**. Records can be created, modified, or deleted without cryptographic proof of who did what, when, and in what order.

2. The DAM Protocol

The Directed Acyclic Mesh (DAM) is formally defined in the Protocol Whitepaper (v0.5.2) as:

M = (Z, V, E, C, π, A)

Where: - **Z** = Zones (autonomous data regions) - **V** = Validation records (cryptographically signed artifacts) - **E** = Causal edges (parent references forming the DAG) - **C** = Classification function (sovereign, restricted, shared, public) - **π** = Partition-merge operator (network split/rejoin handling) - **A** = Analytics layer (queries over the mesh)

Five Formal Properties

1. **Locally flat** — Each zone maintains a complete local view

2. **Globally interconnected** — Zones link via witnessed cross-references
3. **Observer-dependent** — Classification determines what each participant sees
4. **Analytically connected** — Every record is reachable through causal chains
5. **Partition-preserving** — Network splits do not cause data loss or corruption

Five Dimensions

1. **Time** — Monotonic timestamps and causal ordering
2. **Identity** — Post-quantum signatures (Dilithium3 primary, SPHINCS+ backup)
3. **Causality** — Parent references forming a directed acyclic graph
4. **Classification** — Four-tier data sovereignty (sovereign → public)
5. **Witness** — Third-party attestation for cross-zone verification

Post-Quantum Cryptography

All signatures use NIST PQC standards: - **Dilithium3** — Primary signature (lattice-based, 3,293 byte signatures) - **SPHINCS+** — Backup signature (hash-based, conservative security) - **Dual signing** — Every record carries both signatures for defense in depth

3. Architecture

```
┌─────────────────────────────────────────────┐
│              MCP Server (5 tools)            │
├─────────────────────────────────────────────┤
│   ┌──────────┐ ┌──────────┐ ┌──────────┐   │
│   │ Remember │ │  Recall  │ │ Handoff  │   │
│   └──────────┘ └──────────┘ └──────────┘   │
│   ┌──────────┐ ┌──────────┐                 │
│   │  Status  │ │Correction│                 │
│   └──────────┘ └──────────┘                 │
├─────────────────────────────────────────────┤
│           Domain Adapter Layer               │
│  ┌────┐ ┌────┐ ┌────┐ ┌────┐ ┌────┐ ┌────┐ ┌────┐ │
│  │Med │ │Ind │ │Comp│ │Edu │ │Fin │ │Def │ │Agr │ │
│  └────┘ └────┘ └────┘ └────┘ └────┘ └────┘ └────┘ │
├─────────────────────────────────────────────┤
│              Core Protocol                   │
│  ┌──────────┐ ┌──────────┐ ┌────────────┐  │
│  │ L1 Bridge│ │Continuity│ │  Schemas   │  │
│  └──────────┘ └──────────┘ └────────────┘  │
├─────────────────────────────────────────────┤
│         elara-runtime (Rust/PyO3)           │
│  Identity · DAG · Signatures · SQLite       │
└─────────────────────────────────────────────┘
```

Layer Separation

- **Layer 1 (Cryptographic):** `elara-runtime` — Rust implementation providing Identity management, DAG storage, signature operations, and record creation. ~2,700 lines of Rust with PyO3 bindings.
- **Layer 3 (Application):** This system — Python implementation providing domain adapters, memory, corrections, and MCP server. ~3,000 lines.

4. Domain Adapter Pattern

Each domain is a thin adapter (~100-150 lines) on the same protocol foundation:

```python
class DomainAdapter:
    name: str
    compliance_standards: list[str]
    classification_rules: dict[str, Classification]
    record_types: list[str]
```

```python
    threat_vectors: list[str]

    def classify(self, record) -> Classification
    def validate(self, record) -> bool
    def compliance_check(self, record) -> list[ComplianceResult]
```

The adapter pattern means: - **One protocol, seven domains** — No code duplication - **Thin adapters** — Each domain is ~100-150 lines defining schemas and rules - **Pluggable** — New domains added by implementing the base class - **Testable** — Each adapter independently verifiable

5. Domain: Medical

Compliance: HIPAA, GDPR, FDA 21 CFR Part 11

Record Types: - Patient records (SOVEREIGN — never leave origin) - Treatment plans (RESTRICTED — shared with care team only) - Lab results, prescriptions (RESTRICTED) - Anonymized research (PUBLIC)

Validation Rules: - Patient IDs must follow MRN format (MRN-XXXXXXXX) - All records require unique identifiers for audit trail - Cryptographic signatures required per FDA 21 CFR Part 11

Threat Model: - Unauthorized PHI access → Classification enforcement - Record tampering → DAG immutability + dual signatures - Ransomware → Distributed DAG with partition tolerance - Insider threat → Audit trail via causal chain

6. Domain: Industrial

Compliance: ISO 9001, ISO 13485, IEC 62443

Record Types: - Sensor readings (SHARED — distributed monitoring) - Quality reports (RESTRICTED) - Supply chain events (SHARED — multi-party visibility) - Calibration records, maintenance logs (RESTRICTED) - Incident reports (SOVEREIGN)

Validation Rules: - Sensor readings require sensor_id and value - Quality reports require batch_id - Timestamps mandatory for ISO 9001 audit trail - Sensor data must be cryptographically validated per IEC 62443

Threat Model: - Sensor spoofing → Cryptographic validation at source - Supply chain injection → Provenance chain verification - SCADA compromise → Network partition tolerance

7. Domain: AI Companion

Compliance: AI Transparency, Data Sovereignty

Record Types: - Memories (SOVEREIGN) - Corrections (SOVEREIGN) - Handoff state (SOVEREIGN) - Session state (SOVEREIGN)

Key Property: All companion data is classified SOVEREIGN — it never leaves the origin node. This is the original Elara use case: verifiable cognitive continuity.

Validation Rules: - Memories require text content - Corrections require both mistake and correction fields - All data must maintain SOVEREIGN classification

Threat Model: - Memory injection → Content validation + signature verification - Personality drift → Continuity chain detects state deviation - Context poisoning → Hash-chained checkpoints verify integrity - Session hijacking → Identity-bound signatures

8. Domain: Education

Compliance: FERPA, Research Integrity

Record Types: - Student records (SOVEREIGN — FERPA protected) - Research data (RESTRICTED) - Credentials (SHARED — for verification) - Publications (PUBLIC) - Peer reviews (RESTRICTED)

Threat Model: - Grade tampering → DAG immutability - Research fraud → Data provenance chain - Credential forgery → Post-quantum signatures

9. Domain: Finance

Compliance: SOX, PCI-DSS, AML/KYC

Record Types: - Transactions (RESTRICTED) - Account records (SOVEREIGN) - Regulatory filings (RESTRICTED) - Audit logs (SOVEREIGN) - KYC verification (SOVEREIGN) - Public disclosures (PUBLIC)

Validation Rules: - Transactions require amount and currency - KYC verification requires entity_id - Transactions >$10,000 require KYC reference (AML compliance) - All financial records require cryptographic validation (SOX)

Threat Model: - Transaction fraud → Dual-signed immutable records - Money laundering → AML threshold enforcement - Regulatory evasion → Automatic compliance checks

10. Domain: Defense

Compliance: NIST 800-171, CMMC

Record Types: - Secure messages (SOVEREIGN) - Classified documents (SOVEREIGN) - Field reports (RESTRICTED) - Intelligence briefs (SOVEREIGN) - Operation logs (RESTRICTED)

Key Property: Defense records require cryptographic validation AND clearance level designation. Records cannot be PUBLIC or SHARED.

Validation Rules: - All records must be cryptographically signed - Clearance level required on all records - Classification restricted to SOVEREIGN or RESTRICTED only

Threat Model: - Signal interception → Post-quantum encryption resistance - Advanced persistent threats → DAG immutability + partition tolerance - Quantum cryptanalysis → Dilithium3 + SPHINCS+ dual signing - Supply chain compromise → Provenance verification

11. Domain: Agriculture

Compliance: FDA FSMA, GlobalG.A.P.

Record Types: - Sensor readings (SHARED) - Harvest records (SHARED) - Supply chain events (SHARED) - Inspection reports (RESTRICTED) - Pesticide applications (RESTRICTED) - Soil analysis (SHARED)

Validation Rules: - Sensor readings require sensor_id and value - Harvest records require crop and field_id - Supply chain events require origin and destination - Traceability identifier mandatory for all records

Threat Model: - Sensor spoofing → Cryptographic validation - Provenance fraud → Causal chain verification - Label fraud → Immutable harvest-to-retail chain

12. Regulatory Compliance Matrix

Standard	Domain	Key Requirements	DAM Enforcement
			SOVEREIGN classification

HIPAA	Medical	PHI protection, audit trails	SOVEREIGN classification, causal chain
GDPR	Medical	Data minimization, consent	Classification-based access control
FDA 21 CFR 11	Medical	Electronic signatures	Dual post-quantum signatures
ISO 9001	Industrial	Traceability, documentation	Timestamped DAG records
ISO 13485	Industrial	Medical device QMS	Validation records with provenance
IEC 62443	Industrial	Industrial cybersecurity	Cryptographic sensor validation
FERPA	Education	Student record privacy	SOVEREIGN classification
SOX	Finance	Financial reporting integrity	Immutable audit chain
PCI-DSS	Finance	Payment data security	SOVEREIGN account records
AML/KYC	Finance	Transaction monitoring	Threshold-based compliance checks
NIST 800-171	Defense	CUI protection	Post-quantum dual signatures
CMMC	Defense	Cybersecurity maturity	Multi-level classification
FDA FSMA	Agriculture	Food safety traceability	Supply chain provenance chain
GlobalG.A.P.	Agriculture	Good agricultural practices	Validated sensor + harvest records

13. Security and Threat Model

Protocol-Level Defenses

1. **Immutability** — DAG records are append-only. No record can be modified after creation.
2. **Dual Signatures** — Every record carries Dilithium3 + SPHINCS+ signatures. Both must verify.
3. **Causal Ordering** — Parent references prevent record reordering or insertion attacks.
4. **Classification Enforcement** — SOVEREIGN data never leaves origin; RESTRICTED requires explicit consent.
5. **Partition Tolerance** — Network splits handled by the π operator; no data loss on rejoin.
6. **Hash Chaining** — Continuity checkpoints form a verifiable linked list of system state.

Per-Domain Threat Summary

Domain	Primary Threat	Defense
Medical	PHI breach	SOVEREIGN classification
Industrial	Sensor spoofing	Cryptographic validation
Companion	Memory injection	Content + signature verification
Education	Credential forgery	Post-quantum signatures
Finance	Transaction fraud	Immutable audit chain
Defense	Quantum cryptanalysis	Dual PQC signatures
Agriculture	Provenance fraud	Causal chain verification

14. Implementation

The system is approximately 3,000 lines of Python:

Component	Lines	Purpose
core/protocol.py	~300	Layer 1 bridge (optional)
core/continuity.py	~300	Hash-chained checkpoints

core/paths.py	~130	Data directory structure
core/schemas.py	~165	Pydantic validation models
memory/store.py	~200	ChromaDB vector memory
memory/corrections.py	~235	Mistake learning system
memory/handoff.py	~110	Session continuity
hook/hippocampus.py	~200	Context injection hook
domains/ (7 adapters)	~950	Domain-specific logic
server.py	~300	MCP server (5 tools)
cli.py	~65	CLI entry point

Runtime dependency: `elara-runtime` (Rust/PyO3) — 2,700 lines providing Identity, DAG, and cryptographic operations.

Deployment

```
pip install -e .                    # Basic (memory + domains)
pip install -e ".[runtime]"         # With cryptographic validation
elara --domain medical              # Start MCP server
```

15. Cross-References

- **Protocol Whitepaper v0.5.2** — Formal DAM definition, mathematical proofs
- **Hardware Whitepaper v0.1.8** — Tier system for deployment hardware
- **Tokenomics Whitepaper v0.3.2** — Network incentive design

16. Conclusion

The Directed Acyclic Mesh protocol provides a universal foundation for data integrity. By separating the cryptographic protocol (Layer 1) from domain-specific logic (thin adapters), one system serves seven domains with 14 compliance standards. The post-quantum dual signature scheme (Dilithium3 + SPHINCS+) ensures long-term security against quantum threats.

The lean implementation (~3,000 lines) demonstrates that comprehensive data integrity does not require complexity — it requires the right abstractions.
