Lineage-Recorded Provenance

by Nick Clark | Published April 25, 2026

What It Specifies

Each operation's record carries: triggering inputs (with their lineages), operation primitives applied, operation authority, operation outputs (with their lineages flowing forward), and signatures binding the operation. The lineage forms a continuous record.

Lineage retention is governance-credentialed. The retention authority, retention duration, and access controls are declared; the architecture supports the retention requirements that vary by operation class and jurisdiction.

Why It Matters Structurally

Operations without recorded provenance produce architectural opacity. Downstream audit reconstructs from logging that wasn't structured for the audit purpose; the reconstruction is fragile and capture-prone.

Recorded provenance produces structural transparency. The architecture maintains the records; audit traverses the records; the resulting audit is repeatable and verifiable.

How It Composes With Mesh Operation

The architecture defines the lineage-record format, the cross-operation lineage flow, and the retention-and-access primitives. Implementations apply the architecture; provenance operations proceed within the framework.

Lineage composes with all other features. Cross-mesh lineage, byzantine-robust lineage evaluation, and dispute mechanism for lineage disputes all build on the lineage primitive.

What This Enables

Defense audit-grade operations gain structurally-recorded provenance. Civilian critical-infrastructure audit-grade operations gain the same.

The architecture also supports lineage evolution. As audit-grade requirements evolve, lineage protocols update through governance procedures.