

v3.4-LED-003 – Ledger Anchoring, External Verification & Audit Hooks

Document Title	Ledger Anchoring, External Verification & Audit Hooks
Version	v3.4
Document ID	v3.4-LED-003
Date	2025-03-22
Author	Take Back Your Data – Anchoring & Audit Framework
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines anchoring mechanisms, external verification strategies, and audit hook structures for sovereign ledger systems in MaxOneOpen. It ensures that forks can provide external proof without compromising control or sovereignty.

2. Anchoring Strategy

- Anchors are optional but recommended for public traceability
- Anchoring targets: public ledgers, web-of-trust nodes, notary vaults
- Anchors include minimal hash and context envelope
- Anchors must never leak runtime or schema details

3. Verification Layer Structure

Verification Type	Scope	Proof Form
Inline Proof	Local record validation	Hash + schema context
Anchor Proof	External hash publication	Anchor digest w/ timestamp
Federated Proof	Cross-node quorum	Multi-signed claim packet
Regulatory Proof	Read-only mirror	Vault notarized hash extract

4. Audit Hook Implementation

- Hooks must be passive, read-only, and user-approved
- Forks define available audit fields and exposure class
- Audit logs must be exportable with ZK seal or access trace
- No hook may override ledger content or schema policy

5. Certification Triggers

- Anchors must be declared in schema map if used
- Hooks must include visibility trace and proof-of-origin
- External verification must pass reproducibility test
- Certification revoked on tampered or unverifiable hooks

6. Certification Relevance

Only forks with secure, verifiable anchoring and auditable external validation qualify for MaxOneOpen certification. Opaque, unverifiable or centralized audit paths disqualify certification.