

Truth Memory Vaults

Physical Architecture for Ungated Universal Knowledge

Pre-Failure Research Group LLC — Jason D. McCoy

Purpose

Truth Memory Vaults are a physical repository architecture for the Universal Commons — ungated, institution-free, permanently air-gapped storage and access points for knowledge contributed from source.

They exist because any digital, network-connected repository will eventually be captured, corrupted, or controlled. The architecture is designed to make that **structurally impossible**, not merely unlikely.

Node Architecture

The 13 Fixed Nodes

- 13 permanent, physically housed nodes distributed across the world.
- Each node is a complete, self-contained repository — not a mirror, not a shard. Complete.
- **Permanently air-gapped.** No network connection of any kind. No wireless capability. No remote access vector. Physically isolated by design, not by policy.
- **Cannot phone home.** No telemetry, no usage reporting, no external communication of any kind.
- **Physical access only.** All interaction with node content happens on-site, in person.
- Geographic placement criteria (spread, political neutrality, population access, physical security) are still being deliberately resolved — this is a decision the architecture treats as too important to rush.

The 14th Node — The Traveling Node

The 14th node is mobile. It travels physically to each of the 13 fixed nodes on a defined cycle. It is not a backup — it is the integrity and update layer.

- **Sole update path.** New knowledge reaches fixed nodes only through the 14th node, physically delivered. There is no other update mechanism.
- **Physical verification.** Every visit is also a verification event, confirming the fixed node hasn't

been tampered with, captured, or corrupted since the last visit.

- **Interception-proof by design.** Because the only update path is physical and human-carried, there's no network vector to intercept, no remote compromise possible, no supply-chain attack surface for updates.

Core Design Principles

- **Permanently air-gapped** — not a reversible policy, a physical architectural constraint.
- **No central point of capture** — 13 independent complete nodes means no single point of failure, seizure, or control.
- **No gatekeeping** — access to node content is ungated. No credentials, no approval, no institution standing between the individual and the knowledge.
- **Physical integrity verification** — the traveling node's visit cycle is the only trust mechanism. Human, physical, and impossible to spoof remotely.
- **Built for a compromised environment** — the architecture assumes all networked infrastructure is compromised at the protocol level, and simply doesn't trust the network.

The 14th (traveling) node carries new knowledge to each fixed node and verifies that a node hasn't been tampered with since the last visit. The specific verification approach for the traveling node is intentionally left open rather than fixed at this stage.

What's Still Open

Some design questions are deliberately left unresolved rather than forced early:

- Final geographic placement logic for the 13 fixed nodes
- Physical storage medium, access hardware, and housing specification
- Travel cycle frequency and custody-chain protocol for the 14th node
- The contribution protocol — how knowledge enters the commons
- Governance of the traveling-node role, structured to resist capture
- The design of the 14th node itself, including how it verifies integrity on each visit — left fully open for further work

Pre-Failure Research Group LLC | Jason D. McCoy