Avaron, Inc.

Atlanta, Georgia

Anchored Identity Chain System: Decentralized, Tamper-Proof Personal Audit Chains with Global Hash Anchoring and API-Queryable Public Chain Verification

Written by: Chris McWhorter, *CTO, CyberNest Holdings, LLC. Avaron, Inc.*
Date: March 28, 2025

Defensive Publication Title:

Anchored Identity Chain System: Decentralized, Tamper-Proof Personal Audit Chains with Global Hash Anchoring and API-Queryable Public Chain Verification

---

Section 1: Technical Field

This invention relates to secure digital identity systems, distributed ledgers, decentralized logging, forensic traceability, and zero-trust architecture. It presents a novel structure for cryptographically anchored personal audit chains that combine the immutability of blockchain with scalable, private, real-world infrastructure integration.

Section 2: Background of the Invention

Blockchain-based identity and audit systems have faced significant challenges in real-world deployment due to inefficiencies in consensus, data redundancy, privacy exposure, and limited forensic utility. Most current architectures rely on global, fully replicated ledgers that expose user activity publicly and suffer from poor scalability and query performance.

Furthermore, enterprise environments require granular identity-linked audit trails that are immutable, privately controlled, and rapidly queryable in a forensic or compliance scenario — something traditional blockchains do not provide.

There exists a need for a system that:

- Maintains tamper-proof audit logs for each identity.
- Anchors these logs to a global, minimal-verification chain.
- Separates private and public data for privacy-preserving trust validation.
- Enables real-time verification of a user or device's historical actions.
- Allows zero-trust environments to quickly correlate and trace identity activity across infrastructure.

Section 3: Summary of the Invention

The Anchored Identity Chain System consists of:

- **A per-user (or per-device) append-only audit chain**, built using JSON-encoded entries and chained via **Blake3 hashes**.

- Each chain starts with a **Genesis block**, forming a cryptographically verifiable sequence akin to a blockchain but stored privately and off-chain.

- Chains are stored as MinIO objects, organized in folders by **UUID**, and encrypted using the user's **Kyber private key**. Only the user (or trusted device) can decrypt the chain. Recovery is supported via a **16-word key**.

- A **Public Verification Chain** resides on every node. It stores:

    - The Blake3 hash of each user's full private chain.

    - The user's public Kyber key (used for signature validation).

    - Timestamps and meta-information for anchoring updates.

- Prior to any transaction or authentication event, the public chain is queried to validate the integrity of the private chain by comparing the hash.

- An **AI-powered query layer** on core infrastructure nodes parses public chain queries and correlates relationships or anomalies across identities, creating an enterprise-grade forensic engine.

This structure achieves all the benefits of blockchain (immutability, cryptographic trust, historical proof) while avoiding its downsides (public exposure, inefficient consensus, and inflexible data models).

Section 4: Structural Description

4.1 Private Identity Chains

Each user or device is assigned a private, append-only chain beginning with a **Genesis block**, followed by sequential entries, each including a hash pointer to the previous entry.

- **Structure**: Each block is a JSON blob containing:
    - `timestamp`
    - `event_type` (e.g., login, access_granted, file_modified)
    - `event_metadata` (IP, resource ID, command run, etc.)
    - `hash_prev` (Blake3 hash of the previous block)
    - `uuid` (user or device ID)
    - `signature` (signed with user/device's private Kyber key)
- **Chaining Mechanism**:
  Uses a Bitcoin-style approach where each block contains the Blake3 hash of the previous block, creating a one-directional, tamper-evident chain.
- **Storage**:
    - Each chain is stored in a **MinIO bucket** inside a directory named after the user/device UUID.
    - Chains are **replicated and encrypted** using the identity holder's Kyber private key.
    - Only the identity holder can decrypt their chain.
    - A **16-word recovery seed** enables restoration of the decryption key in case of device loss.

4.2 Public Verification Chain

The global, public verification chain is shared across all nodes in the Avaron infrastructure. It serves as a minimal anchoring system for validating the integrity of private chains.

- **Each entry includes**:
    - `uuid` (hashed if privacy is required)
    - `chain_hash` (Blake3 of the current state of the user's chain)
    - `public_key` (Kyber public cert)
    - `last_updated` (UTC timestamp)
    - `signature` (signed by the platform or user/device key)
    - `anchor_id` (for multi-chain references or cross-verification)
- The public chain is **replicated across all nodes** and accessible via an internal API.

Section 5: Verification Logic and API Interaction

1. **Before any transaction**, the platform queries the public chain to:
    - Pull the `chain_hash` and compare it to the local or decrypted chain hash.
    - Ensure the public key used to sign the action matches the stored cert.
    - Check revocation status, expiration, or misalignment.
2. **API Endpoints** allow:
    - Query by UUID or hash.
    - Retrieve the last known hash and timestamp.
    - Audit trail correlation across multiple UUIDs (via AI module).
    - Backwards verification of past chain states for compliance or incident review.

3. **No private data is ever exposed via the public chain.** Only verification data (hashes and keys) are stored globally.

Section 6: Forensic and Enterprise Utility

- **Full-Stack Visibility**: Every interaction, transaction, or config change made by a user or device is traceable to their private chain — which is verifiable at any time via the public chain hash.

- **Tamper Resistance**:
  If any block in a user's chain is modified, the Blake3 chain breaks, and the public anchor no longer matches, flagging the entity as compromised.

- **AI-Driven Correlation**:

    - AI models query the public chain during investigations to identify common infrastructure paths, shared devices, or anomalies in behavior.

    - Temporal and pattern-based analytics can be performed without decrypting any private data — maintaining privacy while still enabling organizational insight.

- **GDPR / HIPAA / Compliance Ready**:

    - Chains can include tagged events (e.g., `gdpr_erasure_request`) to mark erasure points or consent flows.

    - Admins cannot alter logs — only revoke certs or issue access flags.

Section 7: Diagram Descriptions (Textual for IP.com)

Diagram A: Chain Anchoring Overview

Diagram B: Storage Structure

bash
CopyEdit

```
MinIO Bucket: /identity-ledger/
  ├── 6aa9f2d4-1c20-4fd6-b3f7-a1234567890a/
  │   ├── genesis.json
  │   ├── block_002.json
  │   ├── block_003.json
  │   └── ...
  ├── 10cdbfe3-2be9-42cd-9123-abcdef123456/
  │   ├── genesis.json
  │   └── ...
```

Each folder represents a unique user or device ID, fully encrypted and locally stored, with hot replication to Wasabi or S3.

Section 8: Applications and Strategic Impacts

- **Enterprise Identity Protection**:
  Every system interaction is verifiable, reducing insider threat and enabling accountability at the infrastructure level.

- **Blockchain Replacement**:
  This system offers **true immutability without decentralization theater**, providing better performance, privacy, and auditability than traditional blockchains.

- **Zero-Trust Forensics**:
  Forensic teams can reconstruct attack paths or validate config changes across users and time using public chain anchors.

- **Multi-Tenant / MSP**:
  Each tenant maintains their own chains, and MSPs can verify tenant integrity without breaching privacy.

End of Defensive Publication

Inventor: James Christopher McWhorter
Company: Avaron, Inc. | CyberNest Holdings, LLC
Public Disclosure Date: March 28, 2025
Contact: licensing@cybernestit.com