Avaron, Inc.

Atlanta, Georgia

KYC-Anchored Cryptographic Identity Framework with Subpoena-Activated Audit Preservation and Privacy-Preserving Verification Chain

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

Defensive Publication Title:

KYC-Anchored Cryptographic Identity Framework with Subpoena-Activated Audit Preservation and Privacy-Preserving Verification Chain

---

Section 1: Technical Field

This invention pertains to the intersection of decentralized identity systems, blockchain integrity verification, key-based encryption, legal traceability, and privacy-preserving KYC integration. It provides a method for verifiable legal identity anchoring within a cryptographic framework, while preserving the user's privacy, constitutional rights, and control over their private audit trail.

Section 2: Background of the Invention

Most blockchain and decentralized identity systems prioritize anonymity, which creates barriers to law enforcement and forensic accountability. Conversely, identity systems that prioritize traceability often violate user privacy or over-collect sensitive data.

Furthermore, in modern decentralized environments, there is no central authority to process subpoenas or enforce access to encrypted identity chains. This creates tension between user privacy, system integrity, and the legal system's need to enforce valid subpoenas.

The present invention resolves this by:

- Anchoring cryptographic identity to verified KYC providers,
- Recording non-identifiable, hash-linked records on the public chain,
- Allowing legal entities to confirm identity via subpoena **directly with the KYC provider**, and
- Ensuring private data remains encrypted unless lawfully accessed by due process.

Section 3: Summary of the Invention

The system establishes an identity verification and legal traceability framework within a public decentralized identity chain. The key components include:

1. **KYC Provider Integration**
    - A one-time KYC event is performed through an approved provider (e.g., Stripe or Soldfi).
    - The KYC provider assigns a unique internal account number.
    - This account number is hashed using **Blake3** and recorded on the **public verification chain** alongside the user's public key and identity anchor data.
2. **Subpoena Flow (Decentralized Legal Compliance)**
    - Law enforcement (LEO) agencies that receive a valid subpoena can:
        - Query the public chain for a user's anchor hash.
        - Submit the subpoena directly to the **KYC provider** using that hash.
        - The provider hashes its own records and returns the identity match (without needing a centralized intermediary).
    - The public system does not facilitate or investigate on behalf of LEOs; it simply preserves the data integrity and mapping path.
3. **Encrypted Audit Chain Access**
    - Users maintain full control of their encrypted private audit chain (stored in MinIO).
    - Even with a subpoena, the user must either:
        - Provide the decryption key, or
        - Be compelled by the legal process.
    - The platform ensures that the subpoenaed chain cannot be deleted after receipt.
4. **Tamper Logging**
    - Any deletion or modification of the encrypted audit chain after a subpoena is filed is:
        - Logged on the public chain.

        - Flagged with a “chain tampered” status.
        - Made publicly visible to indicate potential evidence tampering.

5. **Subpoena Activation & User Notification**
    - Upon receiving a subpoena, the system:
        - Locks the user’s public verification record from deletion.
        - Prevents removal of the MinIO folder.
        - Notifies the user **within 10 days** of the subpoena filing.

Section 4: System Architecture Overview

4.1 Identity Anchoring Process

- User completes KYC via 3rd party (e.g., Stripe).
- KYC provider assigns internal ID `acct_7890xyz`.
- Blake3 hash of the account ID is generated and recorded:

json
CopyEdit

```
{
  "anchor_hash": "b3b1a9c6f2d21abdb9...",
  "public_key": "kyber768-userkey",
  "uuid": "6aa9f2d4-1c20-4fd6-b3f7-a1234567890a",
  "subpoena_lock": false,
  "chain_status": "active"
}
```

4.2 Public Chain Entry After Subpoena

When subpoena is received:

json
CopyEdit

```
{
  "uuid": "6aa9f2d4-...",
  "chain_status": "locked",
  "subpoena_lock": true,
  "tamper_flag": false,
  "notification_sent": true,
  "notification_due": "2025-04-05T14:00Z"
}
```

4.3 Evidence Destruction Flag

If user deletes or alters chain post-subpoena:

json
CopyEdit

```
{
  "chain_status": "tampered",
  "tamper_flag": true,
  "tamper_detected_on": "2025-04-07T08:32Z"
}
```

Section 5: Privacy, Legal Balance, and Real-World Application

This framework achieves the following:

- **Privacy-Preserving Identity Anchoring**
  Hashes stored on the public chain contain no PII, but can be cryptographically matched by the KYC provider with a valid legal request.

- **Decentralized Subpoena Routing**
  No central platform needs to handle identity release. The blockchain's architecture + KYC provider = full legal traceability.

- **Fourth Amendment Respect**
  Users are not monitored. Their data is not accessed unless:
    - A legal subpoena is issued.
    - Due process is followed.
    - They are legally compelled to decrypt or hand over access.
- **Evidence Integrity Preservation**
  All chains remain encrypted by default. However:
    - MinIO folders cannot be deleted post-subpoena.
    - Attempts to destroy or alter are logged.
    - AI modules can flag anomalies in the chain or timing of deletion.
- **Compliance-Friendly Notification** Users are always notified (within 10 days) that they were the subject of a subpoena — preserving due process and ensuring transparency.

End of Defensive Publication Document

Inventor: James Christopher McWhorter
System Name: KYC-Anchored Identity with Legal Verification Framework
Company: Avaron, Inc. | CyberNest Holdings, LLC
Date of Disclosure: March 28, 2024
Contact: chris@cybernestit.com