**Avaron, Inc.**

*Atlanta, Georgia*

# Tokenized USD Certificates with Burn-on-Use, Paper Redemption, and Biometric Recovery

Written by: Chris McWhorter, *CTO, CyberNest Holdings, LLC. Avaron, Inc.*

Date: March 28, 2025

# Defensive Publication Title:

**Tokenized USD Certificates with Burn-on-Use, Paper Redemption, and Biometric Recovery**

---

## Section 1: Technical Field

This invention relates to digital payment systems, cryptographic identity, decentralized finance, and secure tokenized fiat equivalents. It specifically addresses systems for issuing, transferring, verifying, and redeeming fiat-backed cryptographic certificates in both digital and physical forms, using biometric authentication, public anchoring, and tamper-proof revocation.

---

## Section 2: Background

Conventional fiat systems and modern digital payment platforms (e.g., credit cards, P2P wallets, stablecoins) each suffer from unique drawbacks:

- Credit and debit card systems are susceptible to fraud, chargebacks, and require complex PCI compliance.
- Stablecoins lack consistent transparency, regulatory certainty, and privacy.
- Cash is secure and irreversible, but non-traceable and not digitally portable.

This invention provides a system for securely issuing and managing dollar-pegged cryptographic certificates ("certs") in traditional denominations ($1, $5, $10, $20, $50, $100), combining the strengths of physical cash, digital security, and legal traceability.

---

## Section 3: Summary of the Invention

This system introduces:

1. **Tokenized USD Certs**
    - Represented as **Kyber public/private keypairs** within **signed JSON blobs**.

- Denominations are user-selected and issued via **FDIC-insured accounts** (e.g., through Soldfi).
- Each cert includes:
  - A UUID
  - Amount in clear text
  - Hash of the private key (generated at runtime)
  - Issuer signature
  - Optional redemption metadata

2. **Transfer and Burn Mechanism**
   - Upon use or transfer:
     - The original certificate is **burned** (added to the "Used" log).
     - A **new cert** is issued to the recipient.
     - An **instant API call** transfers funds between FDIC accounts.
   - All transfers use **idempotency tokens** to ensure no duplication or failed transactions.
3. **Revocation and Double-Spend Prevention**
   - All used certs are recorded in a tamper-proof database using **ObjectBox**.
   - Each user device stores a **local copy** of the Used DB.
   - During redemption, the device:
     - Verifies cert integrity
     - Checks the local hash of the DB
     - Confirms the cert has not been spent or revoked (even while offline)
   - Used certs are cryptographically blocked from reuse.

4. **Physical Paper Token Support**
    - Certs can be **printed as paper currency**, containing:
        - A QR code (top-left)
        - Human-readable denomination (top-right)
        - Plain-text private key (bottom)
    - Usable in **offline, off-chain transactions** with basic trust model.
    - Redemption requires **biometric verification via mobile app** to ensure legitimacy.
5. **Biometric Redemption and Recovery**
    - A dedicated mobile app handles:
        - Biometric verification
        - Cert validation
        - Real-time transfer processing
    - Users may trigger **Lost or Stolen Certs** flow:
        - The system checks for unspent certs
        - Destroys them in the Used log
        - Reissues new certs to the user within ~10 seconds

## Section 4: Token Flow Description

### 4.1 Cert Structure (JSON)

```
{
  "uuid": "e9fd0d24-a6b4-4ab7-bde7-1c3ed15bdf52",
  "amount": "$20",
  "key_hash": "blake3_123456abcdef...",
  "issued_by": "avaron_payment_system",
  "signature": "kyber_signed_block",
  "redeemable": true
}
```

---

### 4.2 Cert Issuance Process

1. User deposits funds into FDIC account via Soldfi.
2. User selects denominations.
3. Platform creates one cert per denomination, issues to device over encrypted channel.
4. Public cert + amount + UUID hash are anchored to the **public log** for transparency.

---

### 4.3 Transfer / Use Process

1. User selects cert to spend.
2. Biometric app validates key ownership.
3. Old cert is destroyed (burned + moved to Used log).
4. A new cert is issued to the recipient.
5. API triggers FDIC account transfer in real-time.

---

### 4.4 Offline Verification Process

- ObjectBox DB locally verifies:
    - Token has not been spent
    - Token hash matches amount
    - Device hash is up to date
- If any check fails → transaction rejected
- DB updates when online or manually refreshed

---

### 4.5 Paper Token Redemption

- Recipient scans QR code or enters private key manually
- App performs biometric check of redeemer
- If token is valid and unspent:
    - Burns cert
    - Transfers funds
    - Logs transaction to public chain

---

### 4.6 Lost or Stolen Recovery Flow

- User clicks “Lost or Stolen Certs” in app
- App:
    - Verifies biometric identity
    - Queries public and local Used log

- ○ Flags original certs as burned
- ○ Reissues new certs in same amounts

---

## Section 5: Advantages Over Prior Systems

| Feature | Traditional Cash | Stablecoins | This System |
|---|---|---|---|
| Fraud Protection | ❌ | ❌ | ✅ (biometric verification) |
| Double-Spend Resistant | ❌ | ✅ | ✅ |
| Fully Offline Usage | ✅ | ❌ | ✅ (ObjectBox + printed certs) |
| Instant Recovery | ❌ | ❌ | ✅ (10-second biometric reissue) |
| Traceable Denomination Logs | ❌ | ❌ | ✅ (public anchor log) |
| Real-World Compatibility | ✅ | ❌ | ✅ (printable, scannable) |

---

## End of Defensive Publication

**Inventor**: James Christopher McWhorter
**System**: Tokenized USD Certificates
**Company**: Avaron, Inc. | CyberNest Holdings, LLC
**Date of Disclosure**: March 28, 2025
**Contact**: chris@cybernestit.com