

Blockchain-Based Secure Notarization System (BBSNS)

Project Evolution & Development Report

Duration: July 20, 2025 – February 12, 2026

Current Status: Production Hardening & Final Verification

1. Introduction

This document presents a detailed evolution report of the **Blockchain-Based Secure Notarization System (BBSNS)**. The purpose of this report is to provide a structured overview of how the system architecture matured from its conceptual foundation to its current production-hardened state.

While the earlier synopsis and preliminary reports described the proposed architecture and objectives, the system has undergone multiple structural and security refinements during implementation. This guide documents those technical decisions, architectural pivots, and hardening measures.

2. Phase I – Foundation: Genesis & Tokenomics

(July 20, 2025 – August 31, 2025)

2.1 Initial Objectives

The project was initiated with the following primary goals:

- Develop a blockchain-backed document notarization system.
- Store document hashes on BNB Smart Chain Testnet.
- Implement a token-based ecosystem for notarization workflow.
- Build separate interfaces for Document Owners and Notaries/Admins.

2.2 Dual-Token Architecture

Two ERC-20 based smart contracts were deployed:

- **NTKR (Request Token):** Used by document owners to initiate notarization.
- **NTK (Utility Token):** Used by notaries while processing documents.

The early design focused on base submission cost logic, notary reward/burn patterns, and on-chain transaction traceability. A PostgreSQL schema was created to manage users, documents, token requests, and activity logs.

3. Phase II – Security & Authentication Hardening

(September – October 2025)

3.1 Multi-Factor Authentication Implementation

The authentication model was expanded to include:

- Username + Password
- National ID verification
- Wallet signature verification (**EIP-191** via ethers.js)

Additionally, `express-rate-limit` was integrated, and persistent database tracking of authentication failures was implemented to enforce brute-force protection logic.

3.2 Critical Architectural Decision: Server-Side Hash Authority

Originally, the system allowed client-side document hashing. This approach was revised in October 2025 due to identified vulnerabilities such as submission of falsified hashes and metadata spoofing.

Revised Model: All document hashing moved to backend authority. Backend designated as "Source of Truth." Only server-generated hashes are eligible for on-chain recording.

4. Phase III – Privacy & Audit Integrity

(November – December 2025)

4.1 Task C.4 – Ephemeral File Storage

Previous model: Permanent storage of uploaded documents.

Revised implementation: Original files stored temporarily. Automatic deletion triggered

immediately after notary approval/rejection. Only cryptographic evidence retained (Document hash, Transaction hash, Encrypted summary metadata).

4.2 Task C.5 – Summary Fingerprinting

To prevent silent database tampering, a summary fingerprinting mechanism was introduced:

```
summary_hash = hash(status + notary_wallet + document_hash)
```

This ensures notarization records cannot be modified without detection, providing tamper-evidence even if a database compromise occurs.

4.3 Biometric Liveness Integration

To bind digital identity to real-world identity, **Face API liveness detection** was implemented with dynamic action-based verification and Device-ID tracking for retry continuity.

5. Phase IV – Architectural Modernization

(January 2026)

5.1 Removal of JavaFX-Based Dual Architecture

Initial desktop design (JavaFX + Electron hybrid) created window collisions and redundant UI logic. The decision was made to retire the JavaFX-based UI and move to a **headless backend architecture**.

5.2 Headless Backend & Electron Bridge

The new structure consists of a Node.js (CommonJS) backend API and an Electron + React/Vite desktop interface using a single Chromium runtime and REST communication over localhost.

5.3 Governance Module Introduction

A governance system was added to reduce centralized admin power. High-privilege actions (e.g., banning users) now require structured voting via `governance_proposals` and `governance_votes` tables.

6. Phase V – Production Hardening

(February 2026)

6.1 NTK Mint Overflow Resolution (Feb 11, 2026)

An issue was identified where `DECIMAL(20,18)` was insufficient for larger token values during batch minting audits. The column was expanded to **`DECIMAL(30,18)`** to ensure scalability.

6.2 Rich Metadata Transparency

Added `document_summary`, `rejection_reason`, and integrated direct **BSCScan transaction links** in the UI so users can independently verify on-chain proofs.

7. Summary of Major Decision Changes

Date	Previous Approach	Revised Approach	Rationale
Oct 2025	Client-Side Hashing	Server-Side Hash Authority	Prevent metadata spoofing
Nov 2025	Permanent Storage	Ephemeral Upload Model	Privacy & liability reduction
Jan 2026	JavaFX + Electron	Headless API + Electron Bridge	Architectural simplification
Feb 2026	Basic DB Logs	Summary Fingerprinting	Database tamper detection

8. Current System Status (As of Feb 12, 2026)

- NTKR & NTK contracts verified on BSC Testnet.
- DocumentRegistry contract active.
- 3-Factor Authentication fully operational.
- Face liveness verification integrated.
- Auto-purge file deletion confirmed.
- Governance module functional.
- Desktop application stable in single-instance Electron runtime.
- Mint overflow issue resolved.

9. Conclusion

The BBSNS has evolved from a conceptual blockchain timestamping application into a privacy-conscious, identity-bound, token-governed notarization protocol. The system is currently in a controlled pre-mainnet readiness stage, with emphasis on production stability, audit integrity, and structured decentralization.