Forensic ChainGuard: A Blockchain-Powered Framework for Evidence Integrity

Group-19 Members

Ashish Nadadur Chakravarthi
Kruthi Tirunagari
Shashank Gadipally
Sree Sai Harshitha Nanjyala
Sri Sai Chetana Reddy Janagan

Problem Statement

The traditional approach to managing forensic evidence through chain of custody procedures faces significant vulnerabilities. Manual documentation and centralized databases leave evidence records susceptible to tampering, inefficiency, and human error—all of which can undermine the integrity of evidence presented in court. The Forensic ChainGuard Project offers a modern solution by digitizing this critical process through blockchain technology, creating a secure, transparent, and unchangeable record of evidence throughout its entire lifecycle.

Motivation

This project seeks to transform how we manage forensic evidence by replacing outdated systems with a secure digital alternative. Our primary goal is to rebuild trust in the legal process by establishing a permanent, auditable record of every interaction with evidence - from the moment it's collected through each transfer, examination, and storage event. Blockchain's decentralized architecture provides the foundation for this transformation, strengthening accountability while effectively eliminating the risks of unauthorized tampering or access that plague conventional systems.

Literature Review

Recent research has shown promising results for blockchain applications in maintaining data integrity, enabling traceability, and providing verifiable records without relying on mutual trust between parties. However, practical challenges related to scalability, privacy protection, and implementation costs continue to demand attention. Our examination of Hyperledger Fabric and similar frameworks indicates that permissioned blockchains are particularly well-suited for forensic and legal applications, where privacy controls and regulated access are essential. Current literature highlights several key strategies: using smart contracts to automate record-keeping tasks, implementing encryption to safeguard sensitive information, and employing binary data formats to balance system performance with confidentiality requirements.

Proposed Architecture

The proposed architecture is built on Hyperledger Fabric, a permissioned blockchain framework that supports secure and private transaction processing.

Key components of our system:

- Smart Contracts (Chaincode): Automate evidence lifecycle management (check-in, check-out, transfer, and removal).
- Role-Based Access Control: Ensures only authorized personnel can perform evidence operations.
- AES Encryption: Protects sensitive identifiers like case IDs and evidence IDs.
- Binary Data Storage: Stores blockchain data in binary format for enhanced performance and tamper resistance.
- CLI Interface: Allows authenticated users to perform blockchain operations (add, remove, query evidence).

The architecture ensures full traceability and verification through integrated blockchain integrity checks and historical data access.

Chosen Platform:

The team selected Hyperledger Fabric as the primary framework due to:

- Its support for permissioned networks, allowing strict access control.
- Modular design, enabling customized smart contract development in TypeScript.
- High security through encryption and identity management.
- Private channels for confidential transactions between authorized nodes.
- Seamless integration with Node.js, enabling efficient use of TypeScript's type safety and modern asynchronous features.

The blockchain will be deployed and tested using Docker, with peer nodes (Org1MSP and Org2MSP) connected via a private channel. Deployment will be handled through the Fabric test network, with all dependencies managed via a Linux environment.

References

1. Androulaki, E., et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains: https://arxiv.org/pdf/1801.10228
2. Naveen. "Private Blockchain | Hyperledger Fabric | Getting Started." YouTube, March 21, 2023. https://www.youtube.com/watch?v=rwKPXHUlmks&t=1340s
3. "What Is Hyperledger Fabric? | Blockchain." YouTube, December 5, 2019. https://www.youtube.com/watch?v=iTV89Tqfmgk&list=PLsyeobzWxl7rXr9qxVZPbaoU7uUqP7iPM
4. "Blockchain | Hyperledger Fabric Key Concepts - 1." YouTube, December 7, 2020. https://www.youtube.com/watch?v=BXewrtZoZTo&t=2s
5. Hyperledger. "Hyperledger/Fabric: Hyperledger Fabric Is an Enterprise-Grade Permissioned Distributed Ledger Framework for Developing Solutions and Applications. Its Modular and Versatile Design Satisfies a Broad Range of Industry Use Cases. It Offers a Unique Approach to Consensus That Enables Performance at Scale While Preserving Privacy." GitHub. Accessed May 1, 2024. https://github.com/hyperledger/fabric
6. Hyperledger. "Hyperledger/Fabric-Samples: Samples for Hyperledger Fabric." GitHub. Accessed May 1, 2024. https://github.com/hyperledger/fabric-samples

Team Contract

Roles

- Everyone - **Project Manager**: Oversees progress, ensures milestones are met, and coordinates team communication.
- Kruthi Tirunagari - **Blockchain Developer & Security Specialist:** Implements blockchain structure, cryptographic functions, and designs encryption layers and user authentication mechanisms.
- Ashish Nadadur Chakravarthi - **Backend Developer**: Manages the TypeScript codebase, binary data handling, and integration with Node.js.
- Shashank Gadipally - **System Administrator**: Handles Docker setup, network configuration, and Hyperledger deployment.
- Sree Sai Harshitha Nanjyala - **Frontend Developer & Smart Contract Developer:** Designs user interfaces and assists in smart contract implementation.
- Sri Sai Chetana Reddy Janagan- **Tester & Validator**: Conducts functionality and stress testing of blockchain integrity and smart contracts.

Expectations

The primary objective of the Forensic ChainGuard project is to design and develop a fully functional prototype that demonstrates a secure, transparent, and auditable system for managing forensic evidence throughout its lifecycle. This system must not only replicate but significantly improve upon the traditional paper-based chain of custody process by integrating blockchain technology to ensure data integrity, immutability, and accountability. The following expectations outline the comprehensive scope of deliverables and performance standards for the project:

- Develop a fully functional prototype demonstrating secure evidence management.
- Maintain immutability and transparency across all blockchain transactions.
- Implement AES-encrypted identifiers for data privacy.
- Provide a CLI-based interface for evidence lifecycle operations.
- Achieve seamless interoperability with potential forensic databases and systems.
- Document all installation, configuration, and operational procedures clearly.

Meeting Frequency

The team met twice weekly for progress discussions, coding sessions, and peer reviews.

1. **Weekly Technical Meetings**
   These meetings were held once a week and focused on tracking the progress of ongoing development tasks, resolving technical issues, and coordinating integration efforts across different components of the system. Each session included code reviews, debugging discussions, and short demonstrations of implemented features.
2. **Biweekly Review Sessions**
   Every two weeks, the team conducted in-depth review sessions to assess the overall stability and performance of the blockchain system. These sessions emphasized verifying smart contract reliability, ensuring blockchain synchronization across peers, and maintaining comprehensive project documentation.