Smart Contracts for Government Use: Utilizing Ethereum and Hyperledger Fabric for Ledger Management

CS4991 Capstone Report, 2025

Jake Li
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
qbw2cx@virginia.edu/jakeli1122@gmail.com

ABSTRACT

State-level governments nationwide have experienced an increasing need to digitize paper-based documents, as well as a need for high security to store those documents. To provide a solution for this market, Innova8 LLC and I have proposed two solutions: 1) a secure non-blockchain ledger; and 2) an immutable, secure blockchain ledger. I first utilized the Ethereum blockchain, and its coding language Solidity, to create a naive ledger that could store basic information. After integrating the ledger with the Java end of the project through the Web3j API, I attempted to utilize Hyperledger Fabric to achieve the same result as I did in Solidity but failed to complete the project due to lack of time. I anticipate government workers and citizens of states that purchase the product will benefit, as it will eliminate slow paperwork and offer a quick and efficient document verification process. Future completion of the development utilizing Hyperledger Fabric, a private permissioned blockchain, would lead to greater security.

1. INTRODUCTION

Picture the following: a domestic abuse victim rushes into the police station, fleeing from their abuser. They need to provide identification to the police to receive protection, yet their driver's license, birth certificate, and passport are all locked away at their home - a place inaccessible to them. Law enforcement wants to help; yet without these documents, the process of receiving help and confirming identifying information is slowed, leaving the victim vulnerable in a critical moment. Situations like this highlight the need for a quicker and more secure document management system.

State governments nationwide continue to rely on an outdated, paper-based document storage system, burdening government workers with inefficiencies and citizens with security concerns. In urgent situations like the one described, the lack of a secure, effective, digital system prevents quick verification that can be the deciding factor between safety and danger. The ability to effortlessly and securely store important information digitally - from car registrations to birth certificates - would allow both government workers and citizens to focus on more pressing matters while enabling numerous additional applications.

2. RELATED WORKS

The implementation of blockchain enabled document storage technology has shown promising results in government applications in other countries. As demonstrated by Thailand's National Single Window (THAINSW) gateway implementation, blockchain technology can significantly enhance document security, authentication, and tracking capabilities while reducing operational costs (Thoppae & Praneetpolgrang, 2021). Additionally,

Thoppae's research indicates that blockchain technology is highly suitable for secure document interchange, works effectively with departmental level authority work, and requires strong governmental policy support.

Recent research documented three key relationships between blockchain technology and databases: databases can be used to support and extend blockchains; blockchain features can be used to support and extend databases; and a hybrid exists between them (Kramberger, et. al., 2022). Their analysis reveals that blockchain technology can enhance traditional database management systems by providing improved security features, immutable documentation of transactions, and distributed control mechanisms, highlighting multiple successful implementations in areas requiring high security and transparency, such as identity management systems and access control—applications directly relevant to government document management. This research, specifically on blockchains supporting and extending databases, also aligns with our project's goals of creating a secure document management system that maintains data integrity while providing efficient access, leading to its use as an initial proof of concept.

3. PROJECT DESIGN

This section outlines the technical architecture, implementation strategies and challenges addressed during the development of two blockchain based solutions for government document management: a public blockchain service through Ethereum; and a private, permissible blockchain through Hyperledger Fabric. Additionally, this section explains how the blockchain-based solution extends upon the already established secure, non-blockchain solution. The project design evolved through multiple stages, comparing the positives and negatives of each blockchain service.

3.1 Existing Non-Blockchain Foundation

The project builds upon an existing secure non-blockchain ledger system that serves as the foundation for document storage and management. The system provides a secure storage of actual document content, traditional database architecture with encryption and access controls, hashes produced by encryption used for validation and verification, and more. The blockchain extensions were designed to complement this system by adding immutability and verification capabilities while building upon the existing infrastructure for document storage and retrieval.

3.2 System Architecture Overview

The integrated architecture combines the established non-blockchain system with new blockchain components to create a hybrid solution that maximizes the strengths of each approach. Figure 1 illustrates the high-level architecture of the complete system.

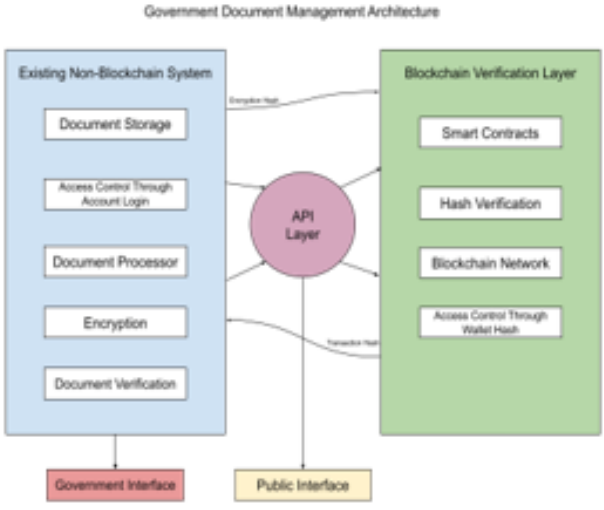

Figure 1: Government Document Management Architecture

Key architectural components include: existing document storage system, blockchain verification layer, an API integration layer connecting both systems, and Government and citizen interfaces.

3.3 Integration with Core System

The blockchain solutions were developed to establish a minimum viable product to show to shareholders. For this purpose, the blockchain implementations were kept initially simple. The smart contract (a program stored within the blockchain) was composed of a few functions: an entry function that allowed the entry of information (such as first name, last name, and an encryption hash); alongside a verification function, which took in parameters to determine if an entry existed.

3.3.1 Ethereum Approach

The Ethereum implementation utilized the public blockchain network to provide transparent verification of the documents while maintaining privacy strategic data management. Our implementation focused on storing document verification metadata rather than actual document content on the Ethereum test network, called Sepolia. The smart contract architecture was written in Ethereum's coding language Solidity and included essential functions for document registration and verification. When documents are registered, only the document hash, timestamp and issuer information are recorded on the blockchain, preserving document privacy while enabling public verification.

Integration with the existing system was facilitated through a middleware layer in Java, ensuring our application was almost entirely Java-based. I utilized the Web3j API to generate Java wrappers for our Solidity smart contract, enabling seamless interaction with the Ethereum Testnet. Through Web3j, I established a connection to the Sepolia network, allowing the application to deploy contracts, send transactions and query necessary blockchain data efficiently. This approach enabled our Java-based application to retrieve and verify information stored on the Ethereum smart contract, ensuring smooth and reliable integration with the core system.

3.3.2 Hyperledger Fabric Approach

To explore a permissioned blockchain alternative, I attempted to implement the same document verification on Hyperledger Fabric (Fabric). The goal was to replicate the functionality of the Ethereum smart contract by developing Fabric chaincode that would store and verify document information in a secure immutable ledger. Fabric was chosen for its suitability in government applications due to features such as permissioned access control, ensuring only authorized individuals could access the blockchain.

I wrote chaincode in Java using the same core logic as the Ethereum contract, implementing functions for document registration and verification. Unlike Ethereum, where smart contracts are written in Solidity, Hyperledger Fabric's chaincode supports multiple programming languages, and I opted to write it in Java, to ensure maximum compatibility with our main application. However, due to time constraints and my lack of familiarity with the technology, the chaincode remained unfunctional.

Despite these challenges, the effort highlighted the potential advantages of Hyperledger Fabric for government applications. Unlike public blockchain solutions, Fabric's permissioned nature allows strict access control, ensuring that only authorized entities can register and verify documents.

3.4 Challenges Faced

Initially, Innova8 and I had to decide between the two blockchain technologies. I researched each technology extensively, concluding that since I had experience with Ethereum, it would be easier to integrate into our project. However, I also concluded that Hyperledger Fabric would be the more suited for our application, as it is private and permissioned. As we had limited time during the internship, we opted to integrate Ethereum into the project first, then revisit Fabric if we

had remaining time. Additionally, when developing using Fabric, there was not much community presence online, leading the learning process to become long and convoluted due to lack of proper learning materials.

4. ANTICIPATED RESULTS

The integration of blockchain-based solutions into government document management is expected to significantly enhance both the security and efficiency of archaic document storage systems. By leveraging Ethereum's public blockchain, the system can provide a transparent verification mechanism while preserving privacy through hashed metadata storage. This will enable government agencies and citizens to quickly verify documents without relying on slow, paper-based processes, thereby reducing processing time. The decentralized nature of Ethereum ensures that once verification data is stored, it cannot be altered, enhancing trust in the verification process.

Once fully implemented, Hyperledger Fabric is expected to offer an even more tailored solution for government applications. With its permissioned structure, Fabric allows only authorized entities to access records, ensuring strict control over more sensitive information. This will mitigate risks associated with public blockchain exposure and eliminate the need for the Cryptocurrency fees associated with Ethereum, while still offering blockchain's immutability and auditing capabilities.

5. CONCLUSION

The implementation of blockchain technology in government management represents a transformative approach to addressing challenges in document storage, verification, and security. By developing both Ethereum and Hyperledger Fabric solutions, this project demonstrated the potential to revolutionize how government agencies handle sensitive documents, offering a more efficient, secure and user-friendly alternative to traditional paper-based systems. The proposed solution addresses critical, real-world scenarios, such as helping domestic abuse victims quickly verify their identity, while providing robust security mechanisms that protect sensitive information. Through careful integration of blockchain technologies with existing secure database infrastructures, the project showcases a practical pathway to modernizing government document management, balancing transparency, privacy and security alike.

6. FUTURE WORK

Future work for this project should focus on completing the Hyperledger Fabric implementation, which was left unfinished due to time constraints during the initial development phase. Specific areas of focus include fully developing the Java-based chaincode, conducting comprehensive security testing, and performing thorough user acceptance trials with government stakeholders. Additionally, further research is needed to optimize the integration between the blockchain verification layer and the existing non-blockchain document storage system. Last, creating user interfaces for both government workers and citizens would be a crucial next step.

7. ACKNOWLEDGMENTS

I would like to thank Amit Sharma, my supervisor for this project.

REFERENCES

Thoppae, C., & Praneetpolgrang, P. (2021). An analysis of a blockchain-enabled e-government document interchange architecture (DIA) in Thailand. TEM Journal, 10(3),1220-1227. https://doi.org/10.18421/TEM103-28

Kramberger, R., Welzer, T., Kamišalić, A. (2022). A preliminary review on complementary applications of databases and blockchain technology. In: Prieto, J., Partida, A., Leitão, P., Pinto, A. (eds) Blockchain and Applications. BLOCKCHAIN 2021. Lecture Notes in Networks and Systems, vol 320. Springer, Cham. https://doi.org/10.1007/978-3-030-86162-9_16