Secure File Sharing System in Collaborative Environments using Block Chain

Dr. Ramesh Cheripelli[1], Matta Sravya[2], Gundeti Sampath[2], Eran.Dharani[2]
[1]*Associate Professor,* [2]*UG Scholar*
Dept. of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad, Telangana, India.chramesh23@gmail.com

***Abstract*—**In collaborative efforts, a group of organizations shares information to create operational synergies. However, centralized file-sharing platforms fail to provide the necessary distributed trust and transparency. Blockchain technology emerges as a solution, offering secure and transparent file-sharing capabilities. This project introduces a blockchain-based system for secure file sharing among consortium members. Utilizing Hyperledger Fabric, an enterprise blockchain framework, the system establishes a blockchain network and implements smart contracts. The Inter Planetary File System (IPFS) is incorporated for distributed file storage. The project delineates workflows for identity management and file-sharing procedures. By leveraging blockchain, the proposed system ensures that organizations within the consortium can exchange files with guaranteed confidentiality, integrity, and availability in a distributed environment.

Keywords*—Block Chain; File Sharing; IPFS: Hyperledger Fabric:*

I. INTRODUCTION

In today's rapidly evolving and interconnected business landscape, collaborative efforts among organizations have become increasingly vital for achieving operational synergies, driving innovation, and maintaining a competitive edge in the global marketplace. As companies seek to leverage their collective strengths and resources, the need for efficient and secure information exchange has grown exponentially. However, traditional centralized file-sharing platforms often fall short in providing the necessary levels of distributed trust, transparency, and security required for effective collaboration across organizational boundaries. This limitation has led to the exploration of alternative technologies that can address these challenges while ensuring secure, efficient, and scalable information exchange. [1,4]

Blockchain technology has emerged as a promising solution to overcome the shortcomings of centralized systems in the context of inter-organizational collaboration. With its inherent characteristics of decentralization, immutability, and transparency, blockchain offers a robust framework for secure and transparent file sharing among multiple parties. By leveraging blockchain's distributed ledger technology, organizations can establish a trustworthy environment for sharing sensitive information without relying on a central authority, thereby mitigating the risks associated with single points of failure and potential data breaches. The decentralized nature of blockchain technology aligns well with the distributed nature of modern business ecosystems, where multiple stakeholders need to collaborate seamlessly while maintaining their autonomy and protecting their intellectual property [2,5]

By providing a shared, tamper-resistant record of all transactions and file exchanges, blockchain enables organizations to establish a common ground of trust, even in scenarios where parties may not have pre-existing relationships or may be geographically dispersed. This project aims to address the pressing need for secure file sharing in collaborative environments by introducing a cutting-edge blockchain-based system designed specifically for consortium members.[3,6]

The proposed solution utilizes Hyperledger Fabric, an enterprise-grade blockchain framework, to create a secure, scalable, and flexible network infrastructure. Hyperledger Fabric's modular architecture and support for permissioned networks make it an ideal choice for consortium-based file sharing, as it allows for fine-grained access control and customizable consensus mechanisms. Additionally, the system incorporates smart contracts to automate and enforce file-sharing protocols, ensuring compliance with predefined rules and access controls. These self-executing contracts not only streamline the file-sharing process but also provide an additional layer of security by enforcing agreed-upon terms and conditions without the need for intermediaries. [7,9]

This automation reduces the potential for human error and malicious activities, further enhancing the overall security and efficiency of the system. To enhance the system's capabilities and address the challenges of distributed file storage, particularly when dealing with large volumes of data, the Inter Planetary File System (IPFS) is seamlessly integrated into the solution. IPFS provides a decentralized approach to storing and retrieving files, complementing the blockchain network's security features and enabling efficient management of large-scale data.[8,10]

By leveraging IPFS, the system can overcome the limitations of storing large files directly on the blockchain, which can lead to performance issues and increased costs. The integration of IPFS with the blockchain network creates a powerful synergy, combining the immutability and transparency of blockchain with the scalability and efficiency of distributed file storage. This hybrid approach ensures that file metadata and access controls are securely recorded on the

blockchain, while the actual file content is stored and retrieved through the decentralized IPFS network. [11,14]

This architecture not only enhances the system's performance but also provides additional redundancy and fault tolerance. The project outlines comprehensive workflows for identity management and file-sharing procedures, ensuring that consortium members can seamlessly interact with the system while maintaining strict security standards. These workflows cover various aspects of the file-sharing process, including user authentication, file upload and encryption, access control management, and secure file retrieval. By implementing robust identity management protocols, the system ensures that only authorized users can access shared files, maintaining the confidentiality and integrity of sensitive information. Furthermore, the proposed system incorporates advanced cryptographic techniques to protect the confidentiality of shared files. End-to-end encryption is employed to secure files during transmission and storage, ensuring that only authorized parties with the appropriate decryption keys can access the file contents.[12,16]

This approach provides an additional layer of protection against unauthorized access and data breaches. By leveraging the combined strengths of blockchain technology and IPFS, the proposed system guarantees confidentiality, integrity, and availability of shared files within a distributed environment. The immutability of the blockchain ensures that all file-sharing activities are recorded in a tamper-resistant manner, providing a comprehensive audit trail for compliance and dispute resolution purposes.

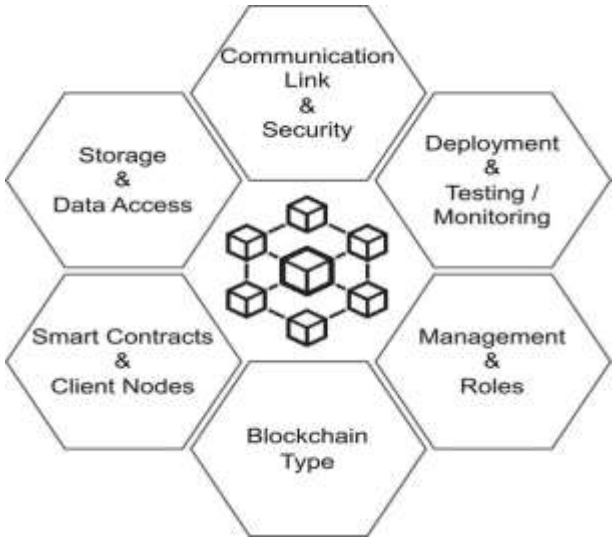

Fig 1: Data Sharing System Model

The decentralized nature of both blockchain and IPFS enhances the system's resilience against single points of failure and potential attacks, ensuring high availability and data durability. This introduction sets the stage for a detailed exploration of the blockchain-based file-sharing system, its underlying technologies, and the potential benefits it offers to consortium members.

The subsequent sections of this paper will delve into the technical architecture, implementation details, security considerations, and performance optimizations of the proposed system. Additionally, the project will address potential challenges and limitations, providing a balanced perspective on the adoption of blockchain technology for secure file sharing in collaborative environments.[13,15,17]

II. RELATED WORK

Blockchain, the foundational technology behind Bitcoin, is fundamentally a technical approach for maintaining a reliable database in a decentralized environment. It employs a blockchain data structure for storing information and utilizes smart contracts for data manipulation and operation. As blockchain technology has evolved, it has found applications in complex scenarios, leading to the emergence of public, consortium, and private blockchains. These variations differ in their number of nodes, level of decentralization, and security requirements.[18]

Public blockchains offer the highest degree of decentralization but suffer from inefficient transactions and limited privacy. Private blockchains, created by single entities, allow for controlled access to data reading, writing, and node addition. However, they have strict limitations on node participation and fewer active nodes. Consortium blockchains, featuring a small number of highly trusted nodes, do not require transaction confirmation from all network participants. They offer advantages such as multi-organizational management, enhanced privacy protection, low transaction costs, and rapid transaction speeds. Consequently, consortium blockchains outperform other types in transaction velocity. Their organization-determined permissions also provide superior privacy protection, making them an ideal choice for data security sharing and trusted governance in the engineering supervision sector.[19,20]

In the realm of blockchain application frameworks, several researchers have made significant contributions. Zhou et al. proposed a comprehensive lifecycle data transaction integration blockchain framework incorporating trust and dispute resolution. Kumar et al. combined blockchain and machine learning to create a trustworthy privacy protection security framework for sustainable smart cities. Makhdoom et al. developed a blockchain-based framework for privacy protection and secure data sharing in smart cities. Quan et al. introduced a trusted medical data-sharing framework utilizing blockchain and outsourcing computing for edge computing. RK et al. presented a blockchain-driven framework with attribute-aware encryption to enhance cloud communication security. Wei et al. proposed a blockchain data access control framework for secure data sharing in the Internet of Things.[21]

As blockchain technology continues to advance, its applications have expanded beyond cryptocurrencies.

Scalability has become a primary research focus, addressing two main aspects: sharing and storage. Research on blockchain scalability from the sharing perspective aims to resolve issues related to lengthy transaction confirmation delays and slow transaction speeds. Storage-level scalability research focuses on reducing blockchain storage costs through data storage-based solutions.[22,23,24]

III. IMPLEMENTATION

In a group of collaborating organizations, data can be shared as files, allowing for operational synergies. A blockchain network established among these organizations requires each participant to maintain an Identity and Interfacing Server (IIS), Smart contract, and blockchain ledger. The IIS stores identity information in a database and serves as the connection point with the smart contract. The smart contract, a program containing the business logic for file sharing, is implemented across all organizations. The blockchain ledger records transactions in block form.

Identity and Interfacing Server

To enable file sharing among users from participating organizations, individuals must register with the blockchain through the smart contract. The end user application generates a key pair (pki, ski). The private key ski remains on the user's device, while the public key and user information (name, email, organization, password, etc.) are transmitted to the IIS. The IIS administrator verifies the user's identity registration request. Upon successful verification, a hash of the password is stored in the identity database.

Blockchain Ledger

The IIS forwards the user registration request to the smart contract, including the public key pki and user details. The smart contract creates a blockchain identifier BCIDi and adds BCIDi, user details, and pki to the blockchain ledger. The blockchain update status (success/failure) and BCIDi are sent back to the IIS. The IIS then communicates the user identity registration status and BCIDi to the end user application.

File Sharing

After blockchain registration, users can securely share files with other registered users. The process begins with user authentication. The user chooses a file to share and specifies the recipients. The end user application creates a symmetric key, K, and encrypts the file, M, using K. The encrypted file M is then uploaded to the IPFS distributed storage. IPFS returns a content ID of the uploaded file, Mcid, to the end user application. The application generates a file identifier, Mfid, for unique file identification. Finally, the end user application requests the public keys of the intended receivers (R1, R2, ...Rn) for file sharing.

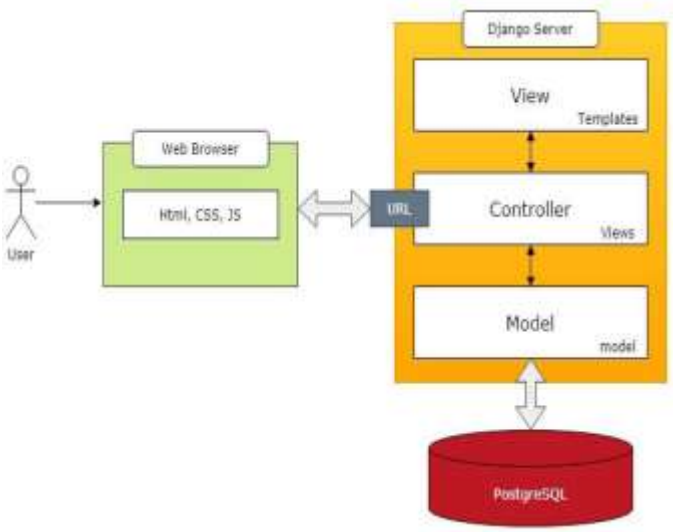

Fig2: Architecture

IV. RESULTS AND DISCUSSION

Engineering construction oversight involves multiple stakeholders, extensive supervision data, and complex information management. Directly implementing blockchain technology for a supervision data-sharing platform presents challenges such as blockchain data storage constraints, privacy concerns in data sharing, limitations in consensus algorithm scalability, and performance issues.

This study introduces a blockchain-based framework for secure engineering supervision data sharing, integrating IPFS for large-scale data storage. A rapid data retrieval system is developed based on the unique storage characteristics of engineering supervision data. The framework incorporates CP-ABE with smart contract technology to enable fine-grained access control for privacy protection. Additionally, smart contracts are designed specifically for engineering supervision data-sharing applications. The framework's security, encryption and decryption processes, and cost-effectiveness are evaluated. Experimental outcomes demonstrate that the proposed framework addresses trust issues among parties involved in engineering supervision data sharing, effectively meets security requirements, ensures traceability of the sharing process, and exhibits high usability and reusability.

The engineering supervision data security sharing system operates primarily within a consortium chain network environment. This setup includes an IPFS network for off-chain metadata storage and a consortium chain network for on-chain summary information storage. Through data sharing, each block node of the supervision party engages in mutual oversight, collectively maintaining the security and consistency of on-chain engineering supervision data. This approach facilitates efficient and standardized management of engineering supervision data and secure sharing applications. Consequently, this article proposes a secure sharing application architecture for engineering supervision data based on a

consortium chain, considering the specific blockchain application scenario.

The architecture comprises five layers: application, contract, interface, consortium chain service, and data storage.

Application layer: This layer implements the data-sharing system based on blockchain, executing transaction functions through client operations. Users can perform tasks such as uploading, querying, and downloading supervision data via the client, subject to permission settings.

Contract Layer: This technical tier facilitates data sharing and transactions on the blockchain network. It manages data uploading, querying, user access control, and smart contract deployment and execution. The contract integrates supervision data sharing requirements, implements access control, and manages the sharing process autonomously.

Interface Layer: Serving as a bridge between the blockchain network and clients, this layer enables client interaction with the blockchain system. It allows for transaction transmission and reception, as well as access to blockchain functions and data.

Consortium Chain Service Layer: Built on a consortium chain, this layer handles ledger status management, consensus management, and blockchain network management. The framework utilizes a decentralized consortium chain implementation, allowing participants to interact with supervision data without relying on third-party trusted institutions, thus enhancing data-sharing efficiency.

Data Storage Layer: This tier stores system-generated data information, comprising three components: blockchain ledger, IPFS distributed file system, and MySQL relational database. In this framework, the data layer primarily stores user information from various participants and essential file data for the supervision business process.

The article proposes a secure sharing framework for engineering supervision data based on a consortium chain. This approach addresses large-scale data storage and transmission challenges in engineering supervision while maintaining blockchain decentralization and enhancing data sharing security. The framework enables secure sharing applications and trusted confidentiality governance of engineering supervision data, effectively meeting the requirements of complex engineering supervision data security sharing applications and trusted management.

However, the process of calculating blockchain node trust degrees and credit ratings involves numerous factors, making it somewhat complex. Future work should focus on streamlining the node calculation method and improving the stability and robustness of the engineering supervision data security sharing application system. Additionally, to expand the framework's applicability to more practical scenarios, further analysis of actual business cases for data security sharing and trustworthy governance is necessary. This will allow for system optimization and integration with existing businesses, showcasing the practical significance and value of blockchain technology in real-world industry applications.

a.

V. CONCLUSION

In conclusion, this paper presents a novel approach to secure file sharing within consortiums by leveraging blockchain technology and distributed storage systems. The integration of Hyperledger Fabric and IPFS addresses the limitations of centralized platforms, providing a robust solution that ensures transparency, trust, and security. By implementing smart contracts and establishing clear workflows for identity management and file sharing, the proposed system offers a practical and efficient method for organizations to collaborate and exchange information. This blockchain-based approach not only enhances the confidentiality, integrity, and availability of shared files but also paves the way for improved operational synergies among consortium members. As organizations continue to seek secure and transparent methods of collaboration, this system stands as a promising solution to meet the evolving needs of inter-organizational file sharing in the digital age.

REFERENCES

[1] Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *18*, 103050.

[2] Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360.

[3] Perera, S.; Nanayakkara, S.; Rodrigo, M.N.N.; Senaratne, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* **2020**, *17*, 100125.

[4] Rahman, M.S.; Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Wang, G. Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1476–1486.

[5] Qin, X.; Huang, Y.; Yang, Z.; Li, X. A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *J. Syst. Archit.* **2021**, *112*, 101854.

[6] Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1146–1160.

[7] Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954

[8] Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653.

[9] Eltayieb, N.; Elhabob, R.; Hassan, A.; Li, F. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. *J. Syst. Archit.* **2020**, *102*, 101653.

[10] Guo, H.; Liang, H.; Zhao, M.; Xiao, Y.; Wu, T.; Xue, J.; Zhu, L. Privacy-Preserving Fine-Grained Redaction with Policy Fuzzy Matching in Blockchain-Based Mobile Crowdsensing. *Electronics* **2023**, *12*, 16.

[11] Ma, X.; Wang, C.; Chen, X. Trusted data sharing with flexible access control based on blockchain. *Comput. Stand. Interfaces* **2021**, *78*, 103543.

[12] Cheripelli, R. and Prasannanjaneyulu, A.N.K, Farmers Market Agricultural Marketing and Management System to Connect Farmers to Retailers, Smart Innovation, Systems and Technologies,2023, volume 363, pages 113-123

[13] Singh, C.E.J.; Sunitha, C.A. Chaotic and Paillier secure image data sharing based on blockchain and cloud security. *Expert Syst. Appl.* **2022**, *198*, 116874.

[14] Agyekum, K.O.-B.O.; Xia, Q.; Sifah, E.B.; Cobblah, C.N.A.; Xia, H.; Gao, J. A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Syst. J.* **2022**, *16*, 1685–1696

[15] Cheripelli, A Blockchain-Based System for the Secure Transfer of Assets,14th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2023-June, pages 885-891.

[16] Cao, B.; Wang, X.; Zhang, W.; Song, H.; Lv, Z. A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain. *IEEE Netw.* **2020**, *34*, 78–83.

[17] Li, T.; Wang, H.; He, D.; Yu, J. Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT. *IEEE Internet Things J.* **2022**, *9*, 15138–15149

[18] Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4177–4186.