ZKG INTERNATIONAL ISSN: 2366-1313

BLOCK-CHAIN BASED INTER ORGANIZATIONAL SECURE FILE SHARING SYSTEM

[1]Mrs. N.V.N. SOWJANYA, [2]T. SAHITHI, [3]GOVINDULA AJAY, [4]P. SATYA KARTHIKEYA

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[2345]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ABSTRACT

An association of entities collaborates and shares data to foster collective efficiencies in their activities. Centralized file-sharing architectures fail to offer decentralized credibility and openness. Blockchain technology offers a solution for secure and transparent file distribution. This document introduces a block-chain-enabled system for secure file exchange across organizations. It is designed for an alliance of entities to exchange files securely in a decentralized manner. Hyper-ledger Fabric, a corporate block-chain platform, is utilized for setting up the block-chain network and crafting smart contracts. The Inter Planetary File System (IPFS) is employed for decentralized file storage. The document outlines the procedures for identity verification and file exchange. The suggested framework enables an alliance of entities to distribute files while ensuring confidentiality, integrity, and accessibility through block-chain. The paper delineates a comprehensive workflow that encompasses identity management and the file-sharing mechanism. Identity management is crucial in establishing trust among the consortium's members, verifying participants, and ensuring that only authorized entities can access the shared files.

1. INTRODUCTION

In response to the growing imperative for cooperative work and data sharing among enterprises, there emerges a call for file-sharing mechanisms that are both secure and transparent. Present-day centralized file-sharing infrastructures fail to meet the requisite standards of trustworthiness and openness, particularly in the context of

sensitive data exchange (Huang et al., 2020). Nonetheless, the integration of blockchain technology can mitigate these issues by facilitating a secure and transparent file-sharing environment across a distributed network. Utilizing Hyperledger Fabric as the foundational blockchain platform, coupled with the Interplanetary File System for decentralized data storage, this innovative system offers a steadfast and effective means for confidential file-sharing within a network of organizations. This system empowers entities within a consortium to exchange files securely through the application of blockchain technology.

The deployment of smart contracts on Hyperledger Fabric allows for the meticulous and secure management of identities and access rights. This guarantees that file sharing and access are confined to verified users, thereby adding an extra layer of security. Moreover, the adoption of multi-signature mechanisms for controlling access further fortifies the security measures for digital assets. In today's globally connected landscape, the necessity for file-sharing systems that are both secure and transparent is escalating among organizations. Conventional centralized file-sharing frameworks are often inadequate in establishing the essential trust and transparency, particularly for the exchange of confidential information. In contrast, blockchain technology presents a viable alternative by enabling a secure and transparent file-sharing process in a decentralized context. This document introduces a blockchain-based system for secure file-sharing across different organizations, designed to support smooth collaboration while safeguarding data security and integrity.

Blockchain technology, which gained prominence with the emergence of Bitcoin, has transformed the approach to recording and authenticating transactions. Each transaction on a blockchain is securely logged and interconnected with preceding transactions via cryptographic methods, ensuring permanence and resistance to tampering. The consensus mechanism, such as Bitcoin's proof-of-work (PoW), allows for transaction verification by network participants, fostering a trustfree setting for data sharing. .Blockchain technology, initially developed for digital currencies, has broadened its scope to encompass a multitude of non-financial functions. Organizations can harness the intrinsic attributes of blockchain, such as immutable record-keeping, openness, and programmable contracts, for diverse

ISSN: 2366-1313

applications like decentralized data repositories and collaborative information dissemination. Nonetheless, when it comes to applications within enterprises, open blockchain networks encounter obstacles like insufficient permissioning and participant responsibility. Consortium blockchains provide an answer by creating a private, regulated network where transactions are confirmed by a select group of recognized nodes, thus maintaining confidentiality and security. .

The architecture utilizes Hyperledger Fabric as the foundational blockchain infrastructure, acclaimed for its extensibility, controlled access, and facilitation of smart contracts. In conjunction with the InterPlanetary File System (IPFS) for decentralized archiving, the architecture offers a solid framework for protected file exchange within a collective of enterprises. IPFS, a distributed peer-to-peer file system, addresses the challenges of blockchain in accommodating substantial data volumes by enabling content-addressable storage solutions. Files on IPFS are retrieved through a unique content-based identifier, guaranteeing an efficient and distributed storage model. Principal elements of the suggested architecture encompass identity regulation via smart contracts on Hyperledger Fabric, certifying that solely validated users can retrieve and disseminate files. The integration of multi-signature protocols augments security by imposing controls on the usage of digital materials.

The system employs IPFS as a proxy for decentralized access governance and collective key administration, facilitating secure and adaptable file distribution among members of the consortium. By marrying the capabilities of blockchain with IPFS, the architecture assures the preservation of data integrity, visibility, and privacy, while bolstering cooperative efforts among organizations. 3 The design capitalizes on Hyperledger Fabric as the core blockchain platform, renowned for its scalability, regulated entry, and support for executable contracts. Paired with the InterPlanetary File System (IPFS) for distributed filing, the design presents a robust structure for safeguarded data transfer among a network of corporations. IPFS, a decentralized peer-to-peer file network, surmounts the limitations of blockchain in handling large data quantities by providing a system of content-referenced storage. By integrating the strengths of blockchain with IPFS, the design guarantees the maintenance of data integrity, transparency, and confidentiality,

ISSN: 2366-1313

while enhancing collaborative interactions among organizations.

2.LITERATURE SURVEY

"Bitcoin: A decentralized electronic cash system," 2008.

A completely decentralized form of digital currency could facilitate direct online transactions between parties without involving a financial intermediary. Although digital signatures offer a solution, their effectiveness is compromised if a trusted third party is still needed to prevent fraudulent spending. We present a remedy for the double-spending issue through a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of proof-of-work based on hashes, creating an immutable ledger that requires redoing proof-of-work to alter. The longest chain not only validates the transaction sequence but also signifies its origin from the largest CPU power pool. As long as the majority of CPU power is held by non-colluding nodes, they will generate the longest chain and surpass attackers. The network operates with minimal organization. Messages are disseminated with the best effort, and nodes have the liberty to enter and exit the network as desired, acknowledging the longest proof-of-work chain as the account of events during their absence. We have proposed a system for electronic transactions devoid of reliance on trust. We commenced with the conventional concept of coins established through digital signatures, which offer robust ownership control but lack a mechanism to prevent double-spending. As long as the majority of CPU power is in the hands of honest nodes, they will maintain the longest chain, thwarting potential attacks. The network operates with minimal structure, relying on nodes' collective efforts. Messages are broadcasted without specific routing, and nodes can freely join or leave, acknowledging the longest chain as the authoritative history. Our system establishes trust less electronic transactions by leveraging digital signatures and a consensus mechanism based on CPU power.

Naz Metal. have developed a secure platform for data exchange utilizing blockchain and the Interplanetary File System. This platform, detailed in their 2019 publication in the journal Sustainability, volume 11, issue 24, article number 7054, offers a robust solution for the secure transmission of data..

Within the academic sphere, the exchange of data is a pivotal activity to maximize

ISSN: 2366-1313

insights from existing studies. Current data exchange platforms are reliant on a central authority, which compromises their reliability, clarity, security, and permanence. Addressing these shortcomings, the discussed document introduces a blockchain-oriented secure platform for data exchange, capitalizing on the advantages of the Interplanetary File System (IPFS). The process begins with the data owner uploading metadata to the IPFS server, which is then partitioned into several confidential segments.

The system ensures security and regulates access by implementing predefined access rules within a smart contract established by the data owner. User authentication is conducted via RSA digital signatures, followed by the submission of a specified fee for the digital content. Post successful data transfer, users are prompted to provide feedback on the data, which is then scrutinized by the Watson analyzer to eliminate any spurious feedback. Contributors of genuine feedback are rewarded, encouraging a comprehensive review process for each file. This model integrates decentralized storage, Ethereum blockchain, cryptographic measures, and a reward system. For practical application, smart contracts are scripted in Solidity and tested on a local Ethereum network. The proposed model delivers transparency, security, controlled access, verification of data ownership, and data quality. Simulation studies evaluate the energy expenditure and the financial implications in USD, providing a realistic cost projection for deploying the system. Additionally, the computational efficiency of various encryption methods is assessed, with Shamir's Secret Sharing (SSS) demonstrating the lowest processing time in comparison to Advanced Encryption Standard (AES) with 128 and 256-bit keys.

Liu J and colleagues authored "BPDS: A Blockchain-Based Privacy-Preserving Data Sharing for Electronic Medical Records," presented at the 2018 IEEE Global Communications Conference (GLOBECOM) on December 9, 2018, spanning pages 1-6, under the auspices of IEEE.

The Electronic Medical Record (EMR) represents a vital category of healthcare information that is garnering significant focus. The dissemination of health-related data is recognized as an essential strategy to enhance the caliber of healthcare services and to curtail the expenses associated with medical care. Electronic Medical Records (EMRs) are currently dispersed among

ISSN: 2366-1313

various independent healthcare facilities, which obstructs the exchange of data and jeopardizes the confidentiality of patient information. To tackle these challenges, we introduce a blockchain-driven, confidentiality-centric data sharing system for EMRs, termed BPDS. Within BPDS, the authentic EMRs are securely housed in cloud storage, while their indices are maintained within an immutable consortium blockchain. This approach significantly diminishes the potential for unauthorized disclosure of medical data, while concurrently ensuring that the EMRs remain unaltered without proper authorization. The automated sharing of data is enabled by the patient-specific access rights embedded within the blockchain's smart contracts. Additionally, the collaborative design of the CP-ABE-based access control and the content extraction signature framework reinforces the protection of privacy in the sharing of data. Security assessments affirm that BPDS offers a secure and proficient method for the sharing of EMR data.

Satapathy U and associates presented "A Secure Framework for IoT Communication Utilizing Hyperledger-Based Blockchain," at the 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) held by IEEE on July 6, 2019

In the contemporary landscape of the Internet of Things (IoT), smart devices are interconnected through both wired and wireless methods. These devices possess the capability to detect environmental parameters and relay this data onward. IoT's realm encompasses Smart cities, Intelligent transport systems, the Healthcare industry, Agriculture, and Environmental monitoring. Within these domains, a substantial amount of data is exchanged between various devices. This data exchange network faces numerous security and privacy issues, such as unauthorized data access, alteration of data, and device authentication. The authors of this paper initially delineate the communication protocols prevalent in IoT applications along with their operational principles. Subsequently, they address the existing challenges within IoT and elucidate the Blockchain-based solutions to these issues. Furthermore, the paper introduces a secure framework founded on an open Blockchain network, designed to mitigate some of the prevalent challenges in IoT applications. It is projected that Blockchain technology will bring about significant transformations in IoT applications shortly.

ISSN: 2366-1313

The vulnerabilities associated with secure communication in IoT applications are tackled by integrating Blockchain technology. The paper proposes a secure communication architecture for IoT Applications, employing a Hyperledgerbased Blockchain system. Within IoT applications, data transmitted by diverse devices is accumulated in a central repository, which poses a risk for security infringements. Moreover, verifying the legitimacy of the data originator is challenging, leaving the system susceptible to security risks. The paper suggests a fortified framework utilizing an open Blockchain (Hyperledger) tailored for IoT environments. The detection of nefarious entities is simplified since each node in the Hyperledger network is cognizant of the others. In essence, this ensures the enforcement of security protocols for non-repudiation, confidentiality, and scalability within an IoT setting.

3. SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE

In a consortium of organizations, a number of organizations can share data in the form files and synergies their operations. A block-chain network created among multiple organizations, each of the organizations will host Identity and Interfacing Server (IIS), Smart contract, and block-chain ledger. IIS maintains the identity details in identity database and is also the interfacing point with the smart contract. A smart contract is a program, which contains the business logic of the proposed file-sharing mechanism, is installed on each of the organizations. The block-chain ledger maintains transactions in the form of blocks. The following Figure illustrates the highlevel view of the proposed system.

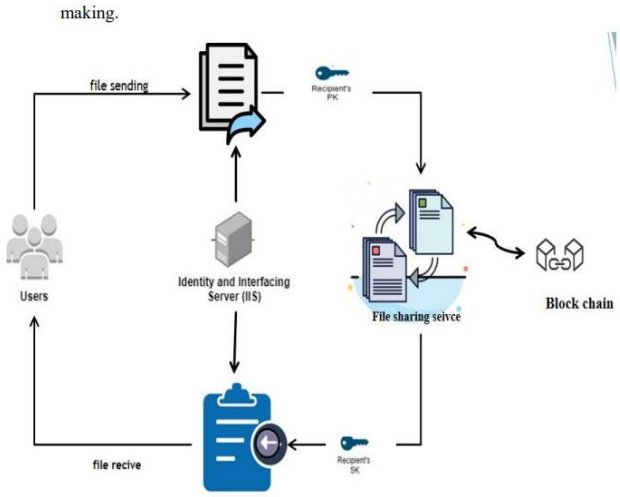


fig 3.1 system architecture

3.2 ACTIVITY DIAGRAM

Activity Diagrams in UML serve to visually represent dynamic workflows, showcasing the sequence and conditions of activities within a system or business process. The key components include nodes, representing actions or decisions, and transitions,

ISSN: 2366-1313

illustrating the flow between these nodes. Initial and final nodes mark the activity's start and end. Control flows connect actions, specifying the order of execution, while decision nodes enable branching based on conditions. Forks and joins manage parallel flows, and swim lanes partition activities among different entities for clarity.

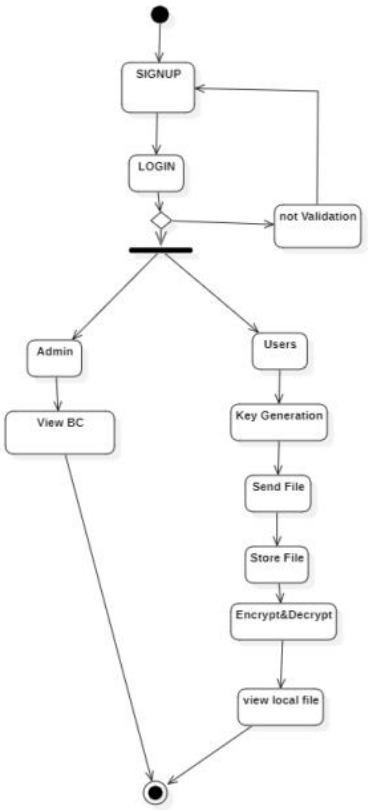
•**Nodes:** Represent actions or decisions.

- **Transitions:** Illustrate flow between nodes.

- **Initial and Final Nodes:** Indicate activity start and end

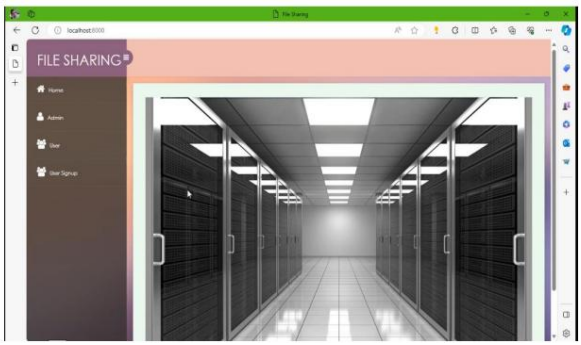
. • **Control Flows:** Connect actions, defining execution order.

- **Decision Nodes:** Facilitate branching based on conditions.



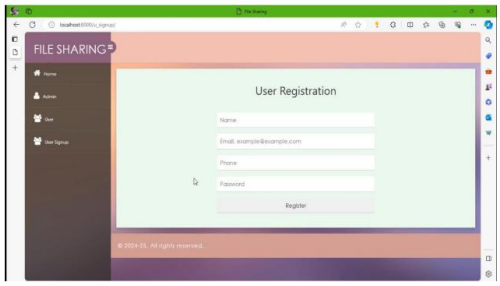
3.2 Represents Activity Diagram

4. OUTPUT SCREENS

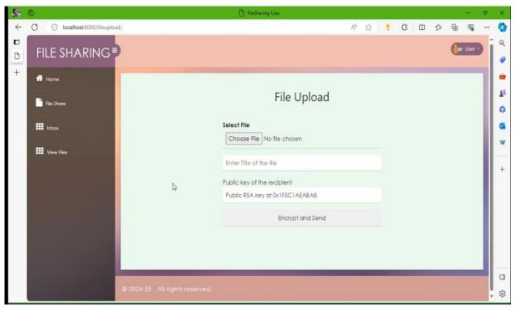


ss 4.1 Home Screen

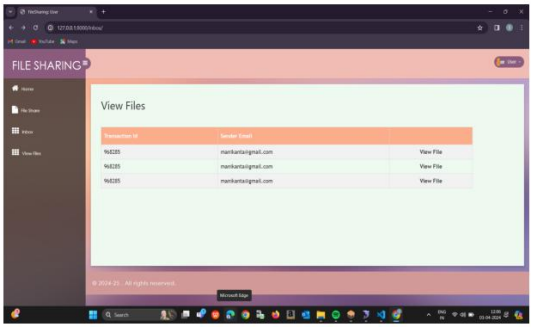
ISSN: 2366-1313



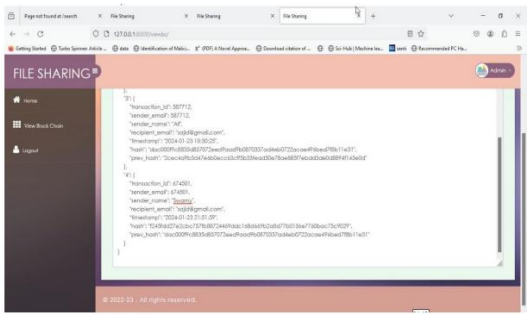
ss 4.2 User Registration



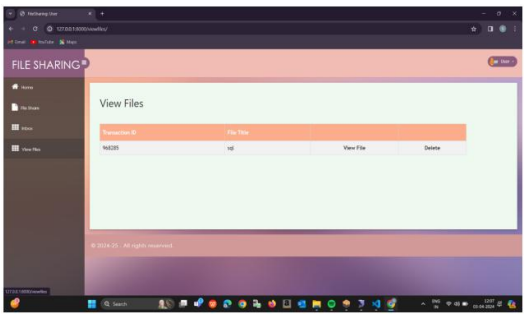
Ss 4.3 Key generation



Ss 4.4 View Files



Ss 4.5 View Data



Ss 4.6 Stored File

5. CONCLUSION

The proposed system provides secure file-sharing across a consortium of organizations using blockchain. It provides confidentiality, integrity, and availability of shared files. It ensures end to end encryption of the files. The content ID of the shared file is stored on the blockchain in a tamper resistant way.This system represents a significant advancement in secure file-sharing, combining the strengths of blockchain and distributed storage technologies to create a decentralized, efficient, and secure framework for inter-organizational collaboration.The encrypted file and file metadata is stored in a distributed fashion on the distributed IPFS storage and blockchain ledger respectively. The system is realized using open source blockchain framework Hyperledger Fabric and tested using Hyperledger Caliper tool.

6. FUTURE ENHANCEMENTS

An innovative enhancement for the project "blockchain-based interorganizational secured file sharing system" could be the integration of decentralized identity management. This enhancement would leverage blockchain technology to provide secure, verifiable, and tamper-proof identities for users within the system. By implementing decentralized identity management, users can maintain control over their personal information while securely accessing and sharing files across organizational boundaries. This enhancement not only enhances security but also promotes trust and transparency among participants in the file sharing network.

7. REFERENCES

1. S. Nakamoto conceptualized "Bitcoin" as a decentralized digital currency system in 2008.
2. Documentation for "Hyperledger Fabric," a blockchain framework, was reviewed in December 2022.
3. M. Naz and collaborators devised a blockchain-interfaced secure data exchange platform, detailed in "Sustainability," issue 24 of volume 11, on December 10, 2019.
4. J. Liu's team introduced "BPDS," a system for safeguarding EMR sharing via blockchain, at the GLOBECOM 2018 event.
5. U. Satapathy's group proposed a secure IoT communication structure using Hyperledger blockchain, discussed at ICCCNT 2019.
6. L. YSari and M. Sipos explored "FileTribe," a blockchain-secured file-sharing system on IPFS, at the European Wireless Conference in 2019.
7. The "Hyperledger Caliper" tool for blockchain performance benchmarking was accessed for documentation in December 2022.
8. The "Apache CouchDB" database system's documentation, version 3.4.0, was perused in December 2022.
9. V. Buterin's white paper in 2014 introduced Ethereum as an advanced smart contract platform.
10. "Bitcoin" is recognized as the pioneering peer-to-peer network for electronic transactions without central oversight.
11. "Hyperledger Fabric" serves as a modular blockchain architecture promoting confidentiality and versatility.

ISSN: 2366-1313

12. The “Sustainability” article by Naz et al. merges blockchain with IPFS for secureλ data stewardship.