Blockchain based secure data sharing platform

by AVCOE Central Library

Submission date: 05-Mar-2025 12:48AM (UTC-0800)
Submission ID: 2582679888
File name: BlockShare_research_paper.pdf (183.91K)
Word count: 3274
Character count: 20172

Blockchain based secure data sharing platform

Prof. K. U. Rahane
rahane_kavita@yahoo.co.in

Mohammadsaani Sayyad
Saanisayyed@gmail.com

Abhijit Sahane
cloudabhi@gmail.com

Sairaj Kankate
sairaj123@gmail.com

Rohit Shinde
rohitshinde0343@gmail.com

Dept. of CE
Amrutvahini College of Engineering
Sangamner, Maharashtra

I. Abstract

In today's digital world, data is incredibly valuable, and ensuring its secure and efficient exchange is more critical than ever. However, centralized data-sharing platforms face significant challenges, including privacy concerns, security risks, data breaches, data loss, and limited user control. These platforms rely on third-party servers and centralized databases, making data vulnerable to misuse, manipulation, and unauthorized access. To overcome these challenges, we propose a decentralized, peer-to-peer (P2P) data-sharing platform inspired by blockchain principles but without the overhead of a full blockchain implementation.

Our system leverages decentralized storage (IPFS) and direct peer-to-peer communication (WebRTC and PeerJS) to enable secure, cost-effective, and efficient data exchange. Unlike traditional centralized models, our platform eliminates intermediaries, ensuring that data remains private, under user control, and resistant to breaches. A message queue system enables offline file retrieval, allowing users to access shared data even when they are temporarily unavailable. Additionally, a unique Peer ID system stored in MongoDB maintains user identity across sessions, enhancing usability and connectivity.

By removing central authorities, BlockShare enables faster, more secure, and highly scalable data-sharing while addressing key limitations of blockchain-based approaches, such as high transaction costs and scalability issues. This innovative model provides a trustworthy, decentralized alternative for individuals and businesses looking to exchange sensitive information securely. Our platform paves the way for a future-proof, privacy-focused, and resilient digital data-sharing ecosystem.

Keywords — Blockchain; Data Sharing; Data Security; Cryptography; Decentralization; Smart Contracts; Secure Communication; Peer-to-Peer; Distributed Ledger

II. Introduction

In today's digital world, data is extremely valuable. Also data is being generated rapidly. This rapidly generated data plays a key role in making decisions, empowering technology, and driving innovation across industries. In today's world data is a new fuel which drives the industries and their operations.

From personal information to important business data, sharing data safely and easily is crucial for everyone including individuals, businesses, governments, and communities that depend on accurate, trustworthy information. But sharing data on these platforms privately and securely remains difficult. Most data-sharing platforms today are centralized, meaning data is stored on a single server or database managed by a third party. While this setup can be convenient and looks secure, it also brings major risks. Centralized platforms are often targeted for hacking, data leaks, data breach and unauthorized access, putting user's information at risk. They also rely on middlemen i.e. some central authority controls the data storage, which can increase costs, reduce privacy, and limit users control over their own data. People using these platforms must trust that their data is safe, but unfortunately, it can still be vulnerable to misuse or loss. [1]

This project aims to solve these problems by creating a secure, private, and efficient data-sharing platform that is different from traditional models. By using ideas from blockchain, such as decentralized storage, and peer-to-peer (P2P) communication. Our platform removes the need for central authorities or central server. Instead of storing data on a centralized server, data is stored in a distributed way and shared directly between users, allowing people to have more control over their information, stronger privacy, and fewer costs. With decentralized storage, like IPFS, data is stored in pieces across different locations, which reduces the risk of data being tampered or data loss. [2]

This platform offers a solution for people and organizations who want to share data securely, without involving third parties or facing high transaction fees. Ultimately, this project redefines data sharing by making it a safe, private, and transparent process. It's a solution that puts user privacy and data security first, helping to create a digital society that is fair, affordable, and secure.

III. Blockchain

Blockchain serves as a foundation for secure, trust-based interactions without the need for a central authority. Blockchain is fundamentally a decentralized digital ledger that stores information across numerous computers, making the data secure and resistant to tampering. Rather than depending on a single centralized system like database or server, blockchain ensures that the information shared between users is reliable, authentic, and remains under the user's control.

Rather than utilizing a traditional blockchain infrastructure, our platform adopts key principles of blockchainsuch as decentralization, security, and peer-to-peer (P2P) data exchange to create a trustless, efficient, and scalable data-sharing system. Instead of maintaining a distributed ledger with immutable transactions, we focus on decentralized storage, direct communication between peers, and an offline message queue system to facilitate secure data exchange. [1]

Directly implementing blockchain for data sharing and storage comes with several challenges that make it impractical for our use case. The primary limitation is the high transaction cost associated with blockchain networks. Public blockchains, such as Ethereum, require users to pay gas fees for every transaction, including data storage and retrieval. These costs can become prohibitively expensive, especially when handling large datasets or frequent data exchanges.

Another critical issue is scalability. Blockchains are designed for consensus-based transaction verification, meaning every transaction must be recorded across multiple nodes, which can significantly slow down the system when handling large volumes of data. This makes blockchain unsuitable for applications that require real-time, high-speed data transfers. Additionally, most blockchain networks have block size and storage limitations, making them inefficient for storing large files directly. Even with solutions like off-chain storage or Layer-2 solutions, the process still involves on-chain metadata transactions, which introduce additional complexity and cost.

Latency is another concern, particularly for real-time data sharing. Since blockchain transactions require validation and consensus from multiple nodes, there is an inherent delay before a transaction is finalized. For a data-sharing platform, where users want to instantly share files, this delay would degrade the user experience.

To overcome these challenges, our platform eliminates the need for a distributed ledger, consensus mechanisms, or smart contracts while still retaining key blockchain-inspired principles like decentralization, peer-to-peer (P2P) communication, and distributed storage. This ensures that our system remains cost-effective, scalable, and efficient, while avoiding the drawbacks of a fully blockchain-based implementation.

IV. Interplanetary File System (IPFS)

The InterPlanetary File System (IPFS) is a decentralized storage that offers a reliable, distributed way to store and share data across the internet. Unlike traditional storage, where data is stored on a single server, IPFS breaks files into smaller pieces and distributes them across multiple computers, or nodes, all over the world. Each file stored on IPFS is assigned a unique identifier known as a Content Identifier (CID), which is like a digital fingerprint for that specific content. Rather than pointing to a location on a server, the CID directly points to the content itself, allowing users to retrieve the file where it is stored. When a file is added to IPFS, it's divided into chunks and stored across different nodes in the network, making the file accessible from multiple sources. If a node holding part of the file goes offline, the data can still be accessed from other nodes, ensuring high availability.

To retrieve a file, users simply use the CID, and IPFS locates the nodes holding that file, allowing it to be downloaded efficiently, often from several sources simultaneously. This decentralized approach means that no single entity controls the user data, giving users greater control and security over their data. [1]

V. Peer-to-Peer (P2P) Network

Using Peer-to-Peer (P2P) network computers can connect directly with each other, instead of going through a central server. In a P2P network, each computer act as both a sender and a receiver, allowing data to share and receive directly between users. This setup is commonly used for sharing files, media streaming, and decentralized applications, where each user can participate equally without relying on a single authority or host. When users want to share data in a P2P network, they simply send it to the intended recipient's computer.

The data doesn't pass through an intermediary server, which makes the transfer faster and often more private. Since there's no central server to store the data, the network is generally more resilient. This also means users have more control over their data, as it doesn't pass through or depend on any third-party provider. Using P2P newtwork, the platform becomes more secure and efficient, supporting private and reliable data sharing that's ideal for a decentralized system [3]

VI. MESSAGE QUEUE SYSTEM

One of the challenges in P2P networks is handling asynchronous communication, where a recipient might not always be online to receive shared data in real time. To address this, we implement a message queue system that temporarily stores file references (CIDs) when the recipient is offline. This mechanism functions similarly to blockchain nodes synchronizing transactions, ensuring that data can still be accessed once the recipient comes online. Instead of storing the actual file in the queue, only the CID is maintained, reducing storage overhead while ensuring that users can still retrieve their files efficiently. By combining IPFS for decentralized storage, P2P communication for direct data exchange, and a message queue for offline handling, our approach preserves the benefits of blockchain decentralization without the transaction fees, scalability limitations, or complexity of traditional blockchain implementations. This creates a lightweight, efficient, and scalable system for secure and seamless data sharing.

VII. LITERATURE SURVEY

Thong Hoang Dilum Bandara Qin Wang Qinghua Lu Xiwei Xu Liming Zhu Petar Popovski Linh T. Nguyen, Lam Duc Nguyen and Shiping Chen. (2023) “Blockchain empowered trust worthy data sharing: Fundamentals, applications, and challenges.” This paper surveys blockchain-based data-sharing architectures, highlighting their transparency benefits while acknowledging challenges like scalability and cost.

Yi Lu, Weichao Wang, Bharat Bhargava, and Dongyan Xu. (2006) “Trust-based privacy preservation for peer-to-peer data sharing.”This paper proposes a trust-based privacy-preservation method for P2P data sharing, where trusted peers (buddies) act as proxies to mask user identity. It also introduces a privacy evaluation method and discusses dynamic trust assessment.

Al-Zahrani Fahad Ahmad. (2020) “Subscription-based data-sharing model using blockchain and data as a service.” This paper proposes a blockchain-based subscription model for secure and fair data sharing, where users pay for data access over time. It introduces different pricing models and demonstrates the feasibility of the approach using a private blockchain network.

Jianping Tu Qimei Jiang Xianggui Yang Pengyong Cao, Guijiang Duan and Chen Li. (2024) “Blockchain based process quality data sharing platform for aviation suppliers.” This paper proposes a blockchain-based platform for securely sharing aviation supplier manufacturing data, addressing data silos and credibility issues. It presents an architecture for quality management, implements security measures, and demonstrates its application in an aircraft industrial park.

Vikas Jaiman and Visara Urovi. (2020) “A consent model for blockchain-based health data sharing platforms.” This paper introduces a blockchain-based consent model for secure health data sharing, using smart contracts to manage and enforce individual consent. It ensures accountability and flexible access control, deploying the model on Ethereum and evaluating different data-sharing scenarios.

Rui Song, Bin Xiao, Yubo Song, Songtao Guo, and Yuanyuan Yang. (2023) “A survey of blockchain-based schemes for data sharing and exchange.” This paper surveys blockchain-based data-sharing and exchange platforms, highlighting their benefits in privacy, security, and interoperability. It analyzes technical architectures, access control, and monetization while reviewing data marketplaces and copyright protection mechanisms.

Min Yang and Yuanyuan Yang. (2014) “Applying network coding to peer-to-peer file sharing” This paper surveys blockchain-based data-sharing and exchange platforms, highlighting their benefits in privacy, security, andinteroperability. It analyzes technical architectures, access control, and monetization while reviewing data marketplaces and copyright protection mechanisms.

peers in different groups to distribute messages for decoding. Moreover, the scheme can be readily extended to support link heterogeneity and topology awareness to further improve system performance in terms of throughput, reliability and link stress. Our simulation results show that the new scheme can achieve 15%–20% higher throughput than another peer-to-peer multicast system, Narada, which does not employ network coding. In addition, it achieves good reliability and robustness to link failure or churn.

VIII. PROPOSE SYSTEM

The proposed system is a decentralized, peer-to-peer (P2P) data-sharing platform designed to eliminate the reliance on centralized servers. By leveraging WebRTC and PeerJS, the system enables real-time, secure, and cost-effective file sharing without transaction fees or third-party control. Unlike traditional platforms that store data on centralized servers, this system enhances data privacy, reduces dependency on cloud storage, and promotes direct communication between users. The core architecture integrates InterPlanetary File System (IPFS) for decentralized storage and a message queue system to facilitate offline data retrieval. This ensures that files remain accessible even when recipients are temporarily unavailable, maintaining seamless and efficient data sharing.

To achieve real-time P2P communication, the platform utilizes WebRTC for direct file and message exchanges without requiring an intermediary. PeerJS Data Channels ensure low-latency and high-speed data transfers, while a lightweight PeerJS signaling server is used only for initial connection establishment, preserving decentralization. The system also incorporates an automated peer discovery and connection management mechanism, which prevents duplicate connections and ensures error handling for seamless interactions. Through this approach, users can securely exchange data without relying on central servers, improving both efficiency and privacy.

For persistent and decentralized storage, the system integrates IPFS, where files are stored in a distributed manner across multiple nodes. Each file is assigned a unique Content Identifier (CID), which acts as a reference for retrieval instead of a traditional URL or database location. This eliminates reliance on centralized storage providers and enhances security by ensuring that files remain tamper-proof and accessible from multiple nodes. If a recipient is online, files are shared directly via P2P communication. However, if the recipient is offline, the file's CID is temporarily stored in a message queue. Once the recipient comes online, they receive a notification and can retrieve the file from IPFS. This message queue system functions similarly to blockchain nodes synchronizing transactions, ensuring that users can access files even when both sender and receiver are not simultaneously available. By storing only CIDs instead of full files, the platform maintains security and efficiency, reducing storage overhead.

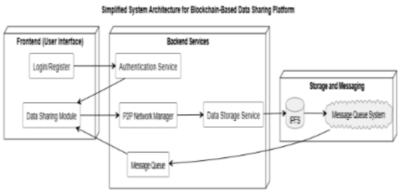

FIG. SYSTEM ARCHITECTURE

To provide user authentication and identity management, the system uses user registration, where each user is assigned a fixed Peer ID. This ensures that users maintain the same identity across multiple sessions, preventing the need to generate a new Peer ID every time they log in. A MongoDB database securely stores user details and assigned Peer IDs, allowing for persistent peer identification and smoother connection establishment. This feature enhances usability and ensures that each user's identity remains consistent, making the data-sharing process more efficient.

The system architecture is designed for both scalability and security. The frontend is built using React.js and Redux, handling user interaction, peer connections, and secure data exchange. The backend consists of a lightweight PeerJS signaling server, MongoDB for user authentication, and a message queue system for offline file retrieval. To enhance data security and privacy, the system implements direct P2P encryption, ensuring that no external entity can access or manipulate the transferred data. Unlike centralized platforms, this system does not store any files in a centralized location, and only decentralized references (CIDs) are maintained, ensuring complete user control over shared data.

By eliminating centralized servers, the proposed system significantly reduces operational costs while enhancing security and privacy. Users have full control over their data, reducing the risks associated with third-party storage.

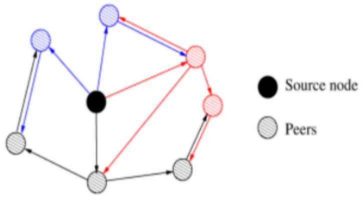

FIG. PEER CONNECTIONS

By integrating WebRTC, PeerJS, IPFS, and MongoDB, the proposed system provides a secure, scalable, and efficient alternative to traditional file-sharing platforms. The decentralized approach minimizes operational costs, eliminates third-party interference, and enhances privacy. Users benefit from real-time file sharing, offline retrieval through message queuing, and a seamless, low-cost data-sharing experience. This architecture makes it an ideal solution for privacy-conscious individuals and organizations seeking a decentralized, secure, and scalable platform for data exchange.

Overall, the proposed system offers a secure, scalable, and cost-effective approach to decentralized data sharing. This innovative approach enhances privacy, minimizes costs, and provides a robust foundation for decentralized applications.

IX. CONCLUSION

BlockShare represents a significant advancement in data privacy, security, and control by shifting away from traditional centralized file-sharing models and embracing a decentralized, peer-to-peer (P2P) architecture. By utilizing IPFS for decentralized storage and direct P2P communication, the platform ensures that users can share files securely, efficiently, and without reliance on third parties. Unlike centralized platforms that store files on controlled servers, BlockShare gives users complete ownership over their data, allowing them to share, retrieve, and verify files independently. Each shared file is assigned a unique Content Identifier (CID), ensuring file integrity, authenticity, and resistance to tampering.

Additionally, the platform includes activity logging mechanisms, allowing users to track sharing history, enhancing transparency and trust within the system. One of the biggest concerns with traditional file-sharing platforms is the risk of data breaches, unauthorized access, and third-party control over user data. BlockShare directly addresses these challenges by removing intermediaries and ensuring that data is exchanged directly between users in a secure manner. The use of message queues for offline data retrieval further improves usability by allowing recipients to access shared files even when they are not immediately available, ensuring seamless and uninterrupted file-sharing experiences. By implementing robust encryption and decentralized identifiers, the platform provides a reliable security framework that minimizes data exposure while maximizing user privacy.

BlockShare not only enhances individual data control but also contributes to a larger shift in digital data exchange towards decentralized, user-centric solutions. It empowers users to manage their digital interactions with confidence, security, and transparency, fostering a trustworthy environment for both personal and business applications. Whether it is for collaboration, secure document sharing, or privacy-focused communication, BlockShare offers a future-proof solution that upholds data sovereignty while ensuring efficiency and accessibility.

Ultimately, BlockShare redefines file-sharing by creating a secure, decentralized ecosystem where users are not dependent on external authorities. By removing centralized points of failure and promoting direct, peer-to-peer interactions, it ensures that data remains private, protected, and under the complete control of the owner. As digital security and data privacy concerns continue to grow, BlockShare sets the foundation for a new era of secure, decentralized, and user-driven data exchange, paving the way for a more private and trustable digital future.

REFERENCES

[1] Thong Hoang Dilum Bandara Qin Wang Qinghua Lu Xiwei Xu Liming Zhu Petar Popovski Linh T. Nguyen, Lam Duc Nguyen and Shiping Chen. Blockchain empowered trust worthy data sharing: Fundamentals, applications, and challenges. NA., 1:40, 2023.

[2] Yi Lu, Weichao Wang, Bharat Bhargava, and Dongyan Xu. Trust-based privacy preservation for peer-to-peer data sharing. IEEE Transactions, 36:498–502, 2006.

[3] Al-Zahrani Fahad Ahmad. Subscription-based data-sharing model using blockchain and data as a service. IEEE Access, 8:115966–115981, 2020.

[4] Jianping Tu Qimei Jiang Xianggui Yang Pengyong Cao, Guijiang Duan and Chen Li. Blockchain based process quality data sharing platform for aviation suppliers. IEEE Access, 11:19007–19023, 2024..

[5] Vikas Jaiman and Visara Urovi. A consent model for blockchain-based health data sharing platforms. IEEE Access, 8(1):143734–143745, 2020

[6] Rui Song, Bin Xiao, Yubo Song, Songtao Guo, and Yuanyuan Yang. A survey of blockchain-based schemes for data sharing and exchange. IEEE Transactions on Big Data, 9:1477–1495, 2023.

[7] Min Yang and Yuanyuan Yang. Applying network coding to peer-to-peer file sharing. IEEE Transactions, 63:1938–1950, 2014.

Blockchain based secure data sharing platform

ORIGINALITY REPORT

12%	9%	9%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	computingnow.computer.org Internet Source	2%
2	Submitted to Glyndwr University Student Paper	2%
3	www.researchgate.net Internet Source	1%
4	Submitted to University of East London Student Paper	1%
5	www.mdpi.com Internet Source	1%
6	arxiv.org Internet Source	1%
7	Fatima Zahra Fakir, Erdem Baydeniz. "The Future of Blockchain in Tourism and Hospitality - Global Insights", Routledge, 2024 Publication	<1%
8	Gaoyuan Quan, Zhongyuan Yao, Longfei Chen, Yonghao Fang, Weihua Zhu, Xueming Si, Min Li. "A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation", Heliyon, 2023 Publication	<1%
9	www.ijcaonline.org Internet Source	<1%
10	Rui Song, Bin Xiao, Yubo Song, Songtao Guo, Yuanyuan Yang. "A Survey of Blockchain-based Schemes for Data Sharing and	<1%

	Exchange", IEEE Transactions on Big Data, 2023 Publication	
11	yingo.ca Internet Source	<1 %
12	Submitted to Swinburne University of Technology Student Paper	<1 %
13	web.comp.polyu.edu.hk Internet Source	<1 %
14	info.daviscollege.edu Internet Source	<1 %
15	Fahim Islam Anik, Nazmus Sakib, Sheikh Iqbal Ahamed. "Integration of blockchain technology into telehealth framework", Elsevier BV, 2025 Publication	<1 %
16	K Karthik, M Kaviya, K Keerthana, M Bhavadharani. "A Survey on Sharing Cloud Data Securely with Encrypted Indexing and User Identity Verification", 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023 Publication	<1 %
17	doaj.org Internet Source	<1 %
18	Irfan Maulana Akbar, Adhitya Bhawiyuga, Reza Siregar. "An Ethereum Blockchain Based Electronic Health Record System for Inter-Hospital Secure Data Sharing", 6th International Conference on Sustainable Information Engineering and Technology 2021, 2021 Publication	<1 %
19	Submitted to University of Birmingham Student Paper	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		