**BlockShare: Blockchain Based Secure Data Sharing Platform**

[[1]](#footnote-1)

Prof. K. U. Rahane Mr. Mohammadsaani Sayyad

✉️[rahane\_kavita@yahoo.co.in](mailto:rahane_kavita@yahoo.co.in) ✉️[Saanisayyed@gmail.com](mailto:Saanisayyed@gmail.com)

Mr. Abhijit Sahane Mr. Sairaj Kankate

✉️[cloudabhi@gmail.com](mailto:cloudabhi@gmail.com) ✉️sairajkankate50@gmail.com

Mr. Rohit Shinde

### ✉️[rohitshinde0343@gmail.com](mailto:rohitshinde0343@gmail.com)

Dept. of CE

Amrutvahini College of Engineering

Sangamner, Maharashtra

# Abstract

The growing reliance on digital data in modern society has made its secure and seamless exchange a top priority. Yet, most current data-sharing platforms depend on centralized systems, which often introduce serious risks — including breaches of privacy, unauthorized access, and limited user autonomy. These centralized models typically rely on third-party servers, making them prone to exploitation and data loss.

To address these vulnerabilities, we introduce BlockShare, a decentralized, peer-to-peer data-sharing solution inspired by the fundamental ideas of blockchain, but without the complexity and cost associated with full blockchain deployment. Our approach combines decentralized storage using the InterPlanetary File System (IPFS) with direct communication channels established via WebRTC and PeerJS. This architecture removes middlemen, empowers users with greater control over their data, and supports efficient file transfers even when one party is temporarily offline — thanks to an integrated message queuing system.

A fixed Peer ID mechanism, stored securely in MongoDB, further enhances the user experience by maintaining consistent identity across sessions. BlockShare not only sidesteps common blockchain drawbacks like high transaction fees and scalability hurdles but also offers a robust, privacy-centric alternative for individuals and organizations seeking secure information exchange. This system lays the groundwork for a more resilient, transparent, and user-controlled digital future.

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

# INTRODUCTION

In the modern digital landscape, data has emerged as one of the most valuable resources. Every moment, vast volumes of data are being created, and this information plays a crucial role in shaping decisions, enabling technological advancements, and fueling innovation across various industries. Much like oil once powered economies, data now drives the digital operations of today’s world.

From sensitive personal details to mission-critical business records, the safe and efficient sharing of data is essential. Whether for individuals, corporations, governments, or research communities, having access to accurate and reliable data is fundamental. However, existing methods for data exchange often lack the privacy and security users expect. The majority of these systems are centralized — meaning that data is stored on servers managed by third-party providers. While such systems may seem convenient, they carry significant risks. Centralized platforms are common targets for cyberattacks, data leaks, and unauthorized intrusions. Moreover, these systems inherently rely on intermediaries, which not only increases operational costs but also strips users of control over their own data. Trusting a third party to keep data secure is not always enough, as breaches and misuse remain ongoing concerns. [1]

To counter these issues, this project introduces a new approach — one that enables secure, decentralized, and user-controlled data sharing. Inspired by blockchain principles, the proposed platform uses decentralized storage and peer-to-peer (P2P) communication to bypass the need for central servers or governing authorities. Instead of storing data in a single location, it is broken into fragments and distributed across multiple nodes, using technologies such as the InterPlanetary File System (IPFS). This method strengthens data integrity and significantly lowers the risk of loss or tampering. [2]

By eliminating third-party involvement, this platform allows users to exchange data directly, affordably, and with confidence in their privacy. It is tailored for individuals and organizations seeking a more secure and transparent way to communicate and share digital information. Ultimately, this project envisions a future where data sharing is not only efficient but also respectful of privacy, cost-effective, and free from centralized control.

# 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 blockchain such 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. [6]

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. [3]

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. [4]

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. [2]

# 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]

# 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 acts 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 network, the platform becomes more secure and efficient, supporting private and reliable data sharing that’s ideal for a decentralized system [7]

# 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.

# 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. [1]

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. [2]

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. [3]

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. [4]

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. [5]

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. [6]

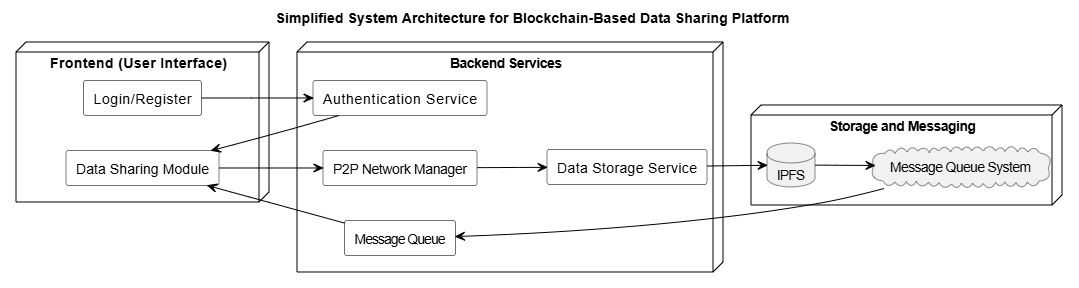
Min Yang and Yuanyuan Yang. (2014) “Applying network coding to peer-to-peer file sharing” The paper proposes a network coding-based peer-to-peer file-sharing scheme that enhances throughput, reliability, and link efficiency by encoding files into multiple messages and distributing them across peer groups. [7]

# Proposed 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. [1]

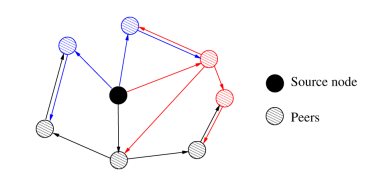


# Fig 1: System Architecture

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.

Fig. 1 represents the system architecture of BlockShare which 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 2: 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, relying solely on peer-to-peer connections without a central server, reduces operational costs, removes third-party interference, and strengthens privacy. Fig. 2 illustrates how peer connections occur in BlockShare. 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. [7]

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.

# 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.
8. Muqaddas Naz, Fahad A. Al-Zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal, and Muhammad Shafiq. A secure data sharing platform using blockchain and Interplanetary File System. *NA.*, 1:40, 2019.
9. Sung-Jung Hsiao and Wen-Tsai Sung. Blockchain-based supply chain information sharing mechanism. NA., 1:40, 2023.
10. Preeti Soni, SK Hafizul Islam, Arup Kumar Pal, Nimish Mishra, and Debabrata Samanta. Blockchain-based user authentication and data-sharing framework for healthcare industries. IEEE Transactions on Network Science and Engineering, 11(4):3623, 2024.
11. Ming Zhang, Zhe Sun, Hui Li, Ben Niu, Fenghua Li, Zixu Zhang, Yuhang Xie, and Chunhao Zheng. Go-Sharing: A blockchain-based privacy-preserving framework for cross-social network photo sharing. IEEE Transactions on Dependable and Secure Computing, 20(5):NA, 2023.
12. Junfang Zeng and Yu Liu. Government data sharing based on blockchain. *NA.*, 1:40, 2023.
13. Mingyue Wang, Yu Guo, Chen Zhang, Cong Wang, Hejiao Huang, and Xiaohua Jia. MedShare: A privacy-preserving medical data sharing system by using blockchain. IEEE Transactions on Services Computing, 16(1):NA, 2023.
14. Afnan M. Alniamy and Hang Liu. Blockchain-based secure collaboration platform for sharing and accessing scientific research data. 2020 3rd International Conference on Hot Information-Centric Networking, 1:40, 2020.

1. [↑](#footnote-ref-1)