World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

# Secure file sharing over block-chain and IPFS

Bhuvaneshwari Shetty *

*Department of Lecturer in Computer Science, Government Polytechnic for Women, Bondel Mangalore, Karnataka, India.*

World Journal of Advanced Research and Reviews, 2021, 12(03), 697-704

Publication history: Received on 19 October 2021; revised on 22 December 2021; accepted on 24 December 2021

Article DOI: https://doi.org/10.30574/wjarr.2021.12.3.0547

## Abstract

Data sharing is a crucial step in the research community to make the most of the prior effort. Platforms for sharing data currently in use rely on trustworthy third parties (TTP). Such systems lack immutability, security, transparency, and trust because of TTP's involvement. In order to address these problems, the proposed system approaches an Interplanetary File System (IPFS)-based blockchain-based secure data sharing platform. The user uploads a data file to the IPFS server, which is subsequently split up into several secret shares. By carrying out the access responsibilities that the user has specified in the smart contract, the suggested scheme accomplishes security and access control. This scenario combines encryption, Ethereum blockchain technology, decentralized storage, and incentive systems. Solidity smart contracts are created and deployed on a local Ethereum test network in order to carry out the suggested scenario. Transparency, Security, Access control, Owner authenticity, and Data quality are all achieved by the suggested plan.

**Keywords:** Block-Chain; IPFS; Secure; Ethereum; TTP

## 1. Introduction

File sharing is a crucial feature for both personal and business use in the current digital world. There are many drawbacks to traditional centralized systems, which handle and distribute data using a single server or data center. These comprise significant hazards to privacy and security, the possibility of data breaches, and vulnerabilities brought on by a single point of failure. The need for more robust and secure data management and sharing techniques is rising as worries about data security and privacy continue to expand.

This investigation looks into, how well the Inter Planetary File System (IPFS) and Blockchain technology can work to alleviate these issues. A decentralized method is provided by blockchain technology, which generates an unchangeable and transparent record that is controlled by a dispersed network of nodes. Through consensus processes, this decentralized structure improves data integrity and security by making it more difficult for unauthorized system to alter or compromise data covertly.

Conversely, IPFS offers a decentralized file sharing and storing system. In contrast to conventional systems that depend on centralized servers, IPFS hosts and retrieves files over a dispersed network. Using a network of nodes to manage data storage and retrieval, this technique not only reduces the risks related to single points of failure but also enhances the effectiveness and resilience of data distribution.

This paper intends to show how Blockchain and IPFS might address the drawbacks of centralized file-sharing systems by analyzing these constraints. This study attempts to illustrate the transformational potential of Blockchain and IPFS by analyzing the drawbacks of centralized file-sharing systems and investigating how these can be resolved. It aims to provide a thorough understanding of how IPFS and Blockchain might improve the distribution of digital material while addressing important issues like scalability, security, and regulatory concerns.

* Corresponding author: Bhuvaneshwari Shetty.

## 2. Optimization in Machine Learning

The approach used in the study of Adel, K. Elhakeem, A, and Marzouk [1] use blockchain technology with the Inter-Planetary File System (IPFS) to investigate a new decentralized system for managing data related to building projects. Using IPFS for effective, distributed file storage and blockchain for safe, transparent record-keeping, their method seeks to solve common project management inefficiencies including information gaps and human error. A blockchain-based solution for Digital Twins (DTs) is presented by Onwubiko, Singh, Awan, Pervez, and Ramzan [2]. Smart contracts are used to improve security and data management by utilizing Ethereum and IPFS. Even with a 10Dr. S. Jayanthy and colleagues [3] developed a blockchain-based system that securely manages patient health data by using IPFS for de-centralized storage and smart contracts for safe transactions and ownership changes. The study by Purnama HMambo[4] offers a novel approach to safe, decentralized IoT data sharing utilizing IPFS and IOTA Tangle. Users may manage their files anonymously and retrieve data quickly with tags, which lowers the requirement for storage. A paradigm for safe multi- group data sharing utilizing IPFS and Hyperledger Fabric is put forth by Feng Wen, Zhi Wang, Limin Qu, Haibo Huang, and Xiapu Hu[5]. It uses dynamic encryption to handle data integrity and key leakage while guaranteeing complete access control for data owners. A safe remote monitoring system based on blockchain technology is proposed by Deepa Rani, Rajeev Kumar, and Naveen Chauhan [6] for patients suffering from chronic illnesses. The system incorporates distributed blockchain technology for data security, IPFS storage, and DApp data administration. By being more efficient and secure than current methods, this strategy improves patient care. Jyotsna Anthal, Shakir Choudhary, and Ravikumar Shettiyar's [7] paper investigates the advantages of blockchain and IPFS technology for safe, decentralized file sharing. It identifies the drawbacks of centralized servers—such as security and privacy concerns—and looks at how blockchain and IPFS can solve these difficulties. The article covers projects like Filecoin and compares other decentralized storage choices like Sia, Storj, and MaidSafe. It comes to the conclusion that while blockchain and IPFS have the potential to transform a number of industries, including digital content distribution, scalability and regulatory issues still need to be resolved. The goal of the study is to present a thorough understanding of these technologies and how file sharing may be affected by them in the future. Harshvadhan, Deepa Kumari, and Abhirath Singh Parmar [8] Using IPFS and Java-enabled GPG encryption, Health Rec Chain is a system for safe medical data storage presented by Sunil Goyal, Kushal Mishra, and Subhrakanta Panda. It has a personalized Ethereum dashboard and a tiered approach that has been put to the test via simulations. Health Rec-Chain outperforms other alternatives in terms of security, privacy, and scalability.

A hybrid blockchain-IPFS system is proposed by Shishu Ding, Hao Hu, Zhenyu Chai, and Wen Wang [9] to improve precast supply chain management's (PSCM) security and efficiency. The solution enhances data privacy and standards through the use of Omniclass-based classification and two-step encryption. Its usefulness for information exchange and implementation is confirmed by a case study. M. Kiran and R. K. Marangappanavar:[10] The difficulties of securely exchanging healthcare data—which frequently involves a number of par- ties, including physicians, patients, researchers, and insurance companies—are discussed in the study. The current approaches are insufficient to guarantee secure data management and preserve patient privacy. The authors suggest combining the Inter-Planetary File System (IPFS) with a blockchain-based architecture to improve the efficiency and security of sharing Personal Health Records (PHR). IPFS enables quicker record retrieval, while Blockchain guarantees tamper-proof data access.

### *Literature gap*

From the literature survey, most of the authors used only IPFS and Block-Chain for sharing or storing of data without using user Freindly development Tools. The contribution of the proposed work is

- Improved security for data files using HASH fuctions and Block-Chain IPFS technology
- Usage of CIA Principle (Confidentiality, Integrity, Authentication), makes it robust
- Pipeline for developing a User freindly tool for better advancement in data Security.

Block-Chain is overely used for securing data but proposed assignment makes use of Hash-function and tools to make data more secure and easily available.

## 3. Proposed Methodology

We developed a fully automated approach for file sharing and storing using Blockchain. The steps involved in the proposed work is depicted in figure 1.

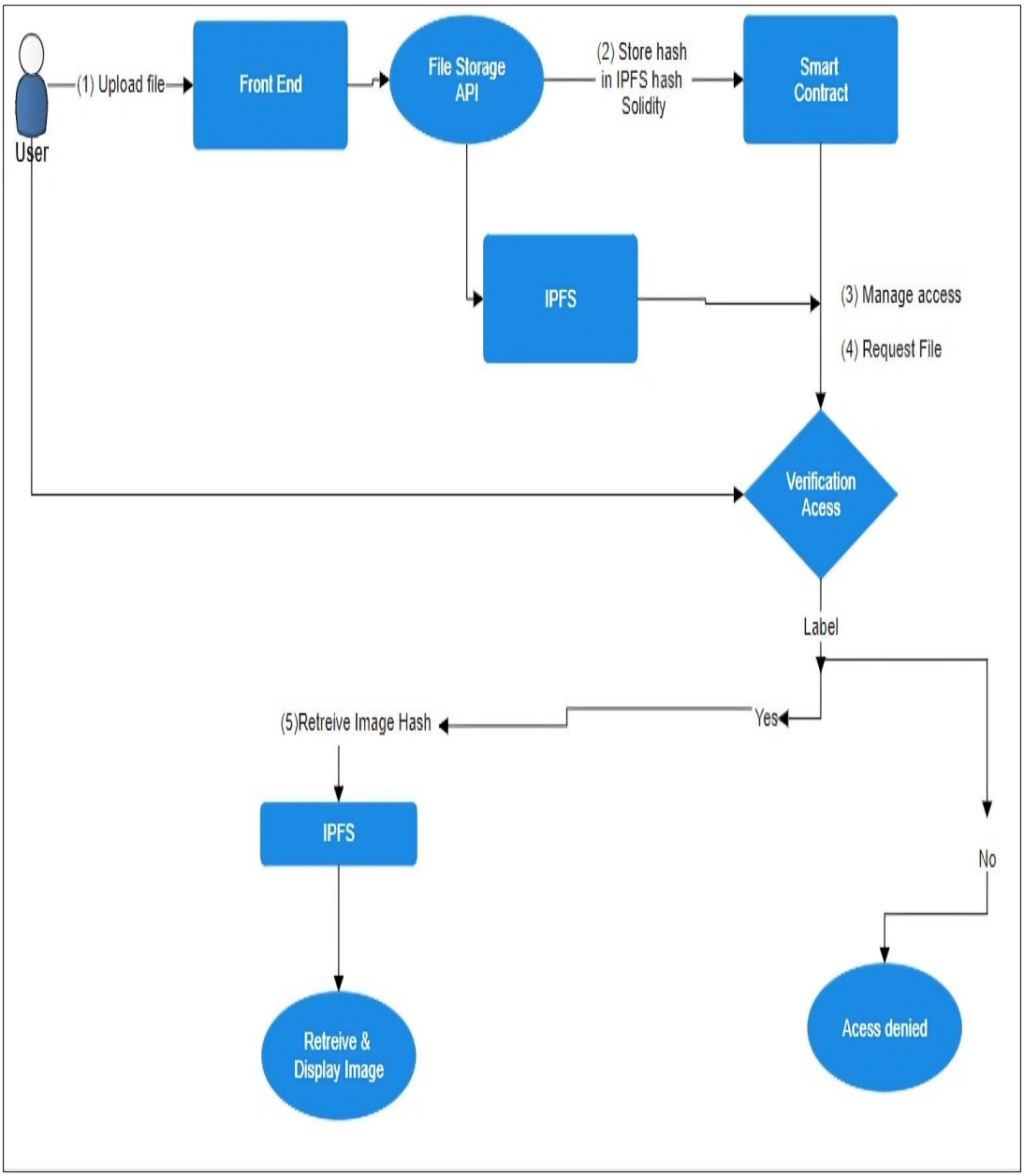


**Figure 1** Work Flow

### 3.1. Picture Transfer

Methodology: The client application starts the picture trans- fer process by using an instinctive user interface that supports file input through HTTP POST demands with multi- part/structure information encoding. This approach empowers the consistent exchange of picture files to the server. The React application use the 'FileReader' API for neighborhood file processing prior to starting the transfer. This nearby taking care of considers proficient processing of huge files and guarantees the honesty of the information being sent. The connection with Pinata's IPFS API includes sending the picture information to Pinata's endpoints, which handle the file ingestion and store the picture on the IPFS network [1].

Go to Web application to transfer Files shown in Fig. 2.

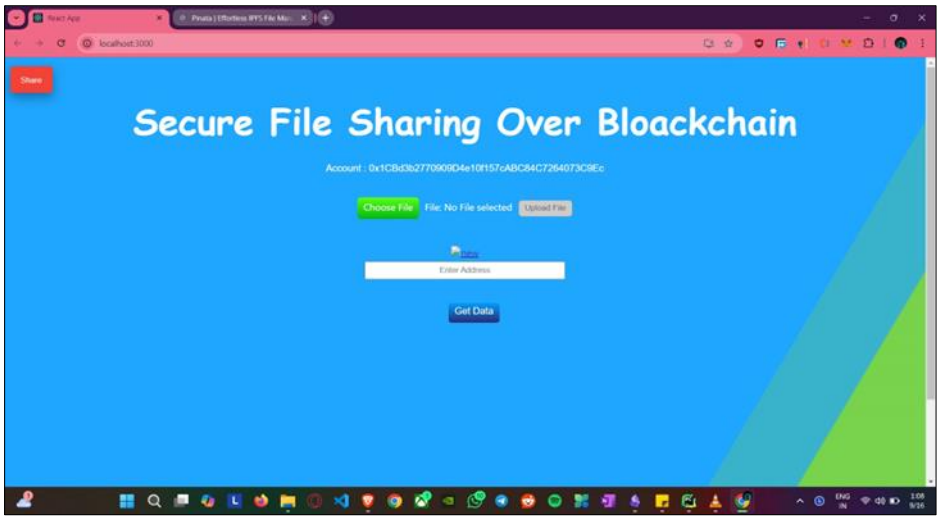


**Figure 2** Adding Account Key

Upload item you want to share in Fig.3

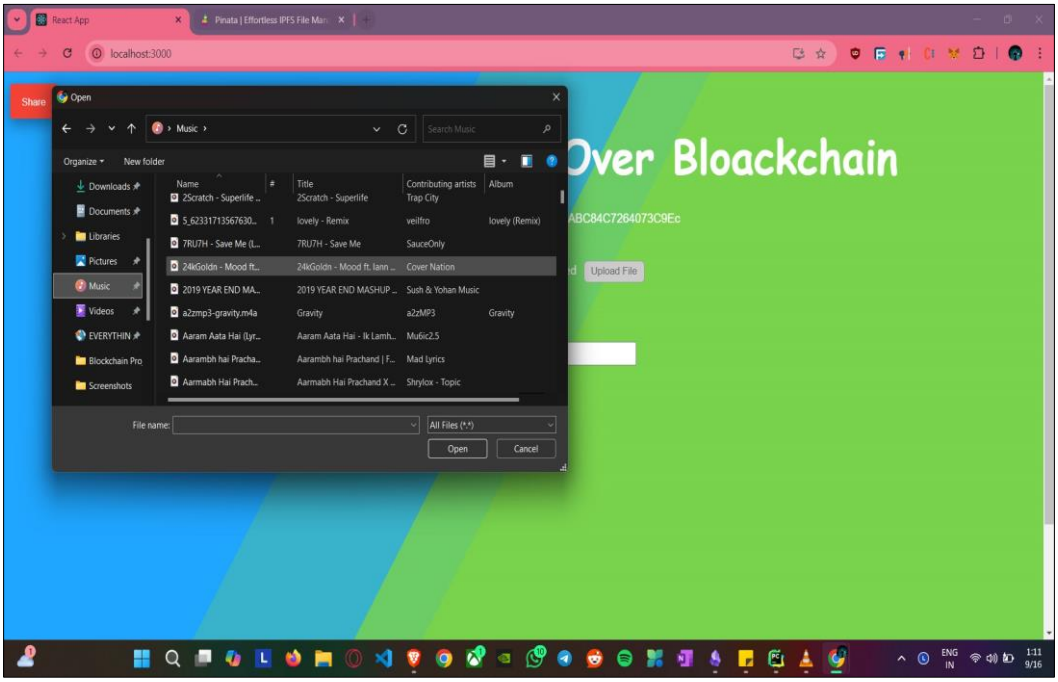


**Figure 3** Adding Account Key

### 3.2. Hash Capacity (IPFS Hash)

When the CID is gotten from Pinata, it is submitted to an Ethereum smart contract through an exchange. This exchange payload is painstakingly developed and marked utilizing Web3 libraries like'ethers.js' or 'web3.js'. The marked exchange is then communicated to the Ethereum organization, guaran- teeing that the information is recorded changelessly on the blockchain. Solidity is utilized to carry out the smart contract rationale, which stores the CID and related metadata (e.g., picture portrayal, transfer timestamp) in the contract's tireless state. This process guarantees that the data is for all time accessible on the blockchain and can be dependably gotten to in the future [5][10].

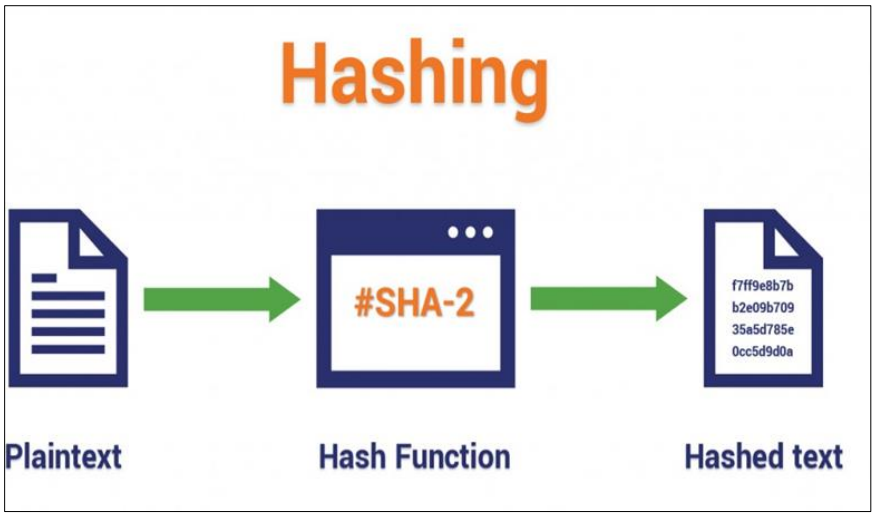


**Figure 4** Hashing method

### 3.3. Access Control

Users oversee access control through smart contract works that change access authorizations. These capabilities are summoned by means of exchanges that use Web3 connection points to associate with the smart contract's inward access control records (leg tendons). The smart contract considers both giving and disavowing authorizations by refreshing log tendons in view of user demands.

### 3.4. Access Confirmation

Access confirmation includes the smart contract checking the mentioning user's location against the consents put away in the leg tendons. The contract evaluates whether the user has the important freedoms to get to the mentioned content in view of predefined access control rules. This process guarantees that main approved users can recover and see the picture. The check incorporates approving the user's location and cross referring to it with the upper leg tendon sections [7][10].

*3.4.1. The proposed system also includes software methodologies like:*

React

- Function: React is used to build the user interface (UI) of the dApp. It enables developers to create dynamic, single-page applications with reusable UI components. React efficiently updates and renders the UI by using a virtual DOM, which improves performance and user experience.
- Role: In a decentralized file-sharing dApp, React manages components for file uploads, viewing files, and interacting with smart contracts. It provides an intuitive and responsive interface for users to interact with the dApp.

Web3.js

- Function: Web3.js is a JavaScript library that con- nects a web application to the Ethereum blockchain. It provides functions for interacting with smart contracts, handling transactions, and retrieving blockchain data.
- Role: In the dApp, Web3.js is used to call smart contract functions, send transactions to store file metadata on the blockchain, and query data from the Ethereum network. It interfaces with MetaMask to manage user accounts and transactions.

Pinata

- Function: Pinata is a service that provides reliable pinning and management of files on IPFS. IPFS is a decentralized file storage network that ensures files are distributed across nodes.
- Role: Users upload files to IPFS through Pinata, which pins the files to ensure they remain accessible. The dApp uses Pinata's API to upload files, retrieve their IPFS hashes, and manage file metadata. This approach ensures file persistence and decentralization.

MetaMask

- Function: MetaMask is a cryptocurrency wallet and gateway to blockchain applications. It allows users to manage their Ethereum assets and interact with dApps directly from their browser.
- Role: MetaMask is integrated into the dApp to handle user authentication and transaction signing. It provides a secure way for users to connect their Ethereum wallets, approve transactions, and interact with the dApp's blockchain features.

### 3.5. Methodology involved in Recovering Image

*3.5.1. Recover Picture Hash*

In the event that the smart contract awards access, the front-end application utilizes the returned CID to give a GET solicitation to an IPFS entryway. This solicitation recovers the picture information from IPFS utilizing the conveyed hash table (DHT) to find the substance inside the decentralized organization. The front-end application handles the information recovery and sets it up for rendering in the user interface [6][4].

*3.5.2. Getting Image*

The picture is shown to the user assuming access is approved. Assuming there are issues with access or information recovery, suitable blunder messages are introduced, guaranteeing that the user is educated regarding any issues

## 4. Result and Discussion

The Full-Stack Decentralized File Sharing dApp has been thoroughly assessed through both subjective and quantitative measures. The accompanying results have been noticed:

- Improved Security: The execution of blockchain innovation has effectively guaranteed that all file exchanges are recorded permanently. This has successfully limited chances related with information altering and unapproved access. Cryptographic strategies have been utilized to get user information, showing strong assurance against expected breaks.
- Further developed Protection: The decentralized idea of the dApp permits users to hold command over their own information. Dissimilar to conventional file-sharing systems that frequently depend on unified servers, this dApp guarantees that users' very own files are disseminated across a distributed organization, lessening the probability of information double-dealing by outsiders.
- Expanded Effectiveness: Execution benchmarks show that file transfer and download speeds are practically identical to, while perhaps worse than, customary concentrated systems. The disseminated network design has been advanced to deal with huge volumes of information without critical inertness, exhibiting the system's versatility.
- User Experience: The user interface has been planned in view of straightforwardness and instinct. User input has been predominantly certain, with specific applause for the simplicity of route and consistent reconciliation of file the board highlights. The system's full-stack approach guarantees a durable encounter from the frontend to the backend.
- Adaptability: The dApp has shown to be profoundly versatile. Tests directed with changing quantities of users and information loads showed that the system keeps up with execution and dependability, supporting a developing user base without corruption in help quality.

### 4.1. Retrieval of Data

Sharing the file using account key.

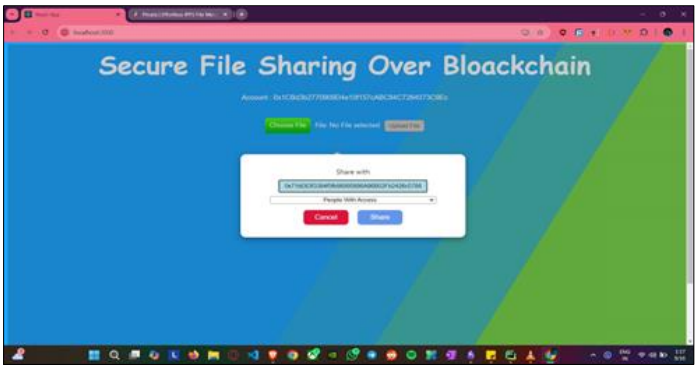


**Figure 5** Adding Account Key

If access has assured then enter 'get data' shown below in fig.6.

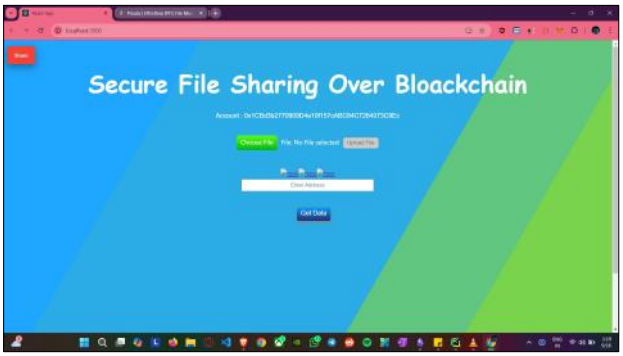


**Figure 6** Data Retrieval

The retrieved file can be downloaded as shown in Fig.7.

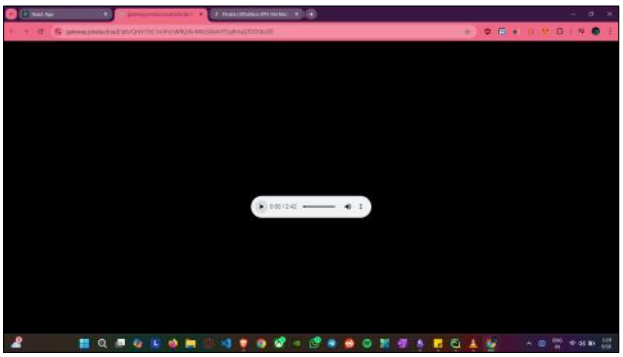

**Figure 7** Data Produced

### 4.2. Difficulties and Future Bearings:

In spite of the promising outcomes, a few difficulties remain. For example, while the dApp has major areas of strength for exhibited and security, progressing endeavors are expected to address possible weaknesses as the innovation develops. Furthermore, user instruction on decentralized systems is important to understand the advantages of such stages completely. Future improvement ought to zero in on further upgrading security highlights, investigating progressed blockchain conventions, and enhancing execution for much bigger sizes of activity. Proceeded with commitment with users and iterative enhancements will be pivotal in refining the system and guaranteeing its drawn out progress.

## 5. Conclusion

The proposed work has applied Block chain and Ipfs to share files. The Full-Stack Decentralized File Sharing d App represents a significant advancement in the realm of digital file management, leveraging the power of decentralized technologies to provide a more secure, transparent, and efficient platform for users. By utilizing blockchain and peer-to-peer networks, this system addresses many of the inherent limitations of traditional centralized file sharing methods, including issues of security, privacy, and data control. The integration of blockchain ensures that file transactions are immutable and verifiable, fostering trust and integrity within the network. Meanwhile, the peer-to-peer architecture decentralizes data storage and distribution, minimizing the risk of single points of failure and reducing reliance on intermediaries. This approach not only enhances security but also improves accessibility and scalability, accommodating a growing user base with varied needs.

## References

[1] Adel, K. Elhakeem, A., Marzouk, M. (2023). Decentralized system for construction projects data management using blockchain and IPFS. Journal of Civil Engineering and Management, 29(4), 342–359.

[2] Austine Onwubiko, Raman Singh, Shahid Awan, Zeeshan Pervez and Naeem Ramzan. School of Computing, Engineering and Physical Sci- ences, University of the West of Scotland, Paisley PA1 2BE, UK Sensors 2023, 23(14), 6641.

[3] Dr. S. Jayanthy, A. Arunkumar, Mr. J. Judeson Antony Kovilpillai, M. Bhuvardhena, K. Dinesh Pandian, Secured Health Data Sharing System using IPFS and Blockchain with Beacon Proxy, Procedia Computer Science, Volume 230,2023,Pages 788-797,ISSN 1877-0509

[4] Purnama, H.; Mambo, M. IHIBE: A Hierarchical and Delegated Access Control Mechanism for IoT Environments. Sensors 2024, 24, 979.

[5] Wen F, Wang Z, Qu L, Huang H, Hu X. 2024. Enhancing secure multi- group data sharing through integration of IPFS and hyperledger fabric. PeerJ Computer Science 10:e1962

[6] Rani D, Kumar R, Chauhan N. A secure framework for IoT-based healthcare using blockchain and IPFS. Security and Privacy. 2024; 7(2):e348.

[7] Jyotsna Anthal, Department of Information Technology, Thakur Col- lege of Science and Commerce, Mumbai, India. Shakir Choud- hary, Department of Information Technology, Thakur College of Science and Commerce, Mumbai, India. Ravikumar Shettiyar, Department of Information Technology, Thakur College of Science and Commerce, Mumbai, India (2023 International Conference on Advancement in Computation Computer Technologies (InCACCT)

[8] Smart GAN: a smart generative adversarial network for limited imbalanced dataset 2024, Journal of Supercomputing. A healthcare data management system: Blockchain enabled IPFS providing algorithmic solution for increased privacy preserving scalability and interoperability 2024, Research Square. A Manifesto for Healthcare Based Blockchain: Research Directions for the Future Generation 2024, Journal of The Institution of Engineers (India)

[9] Secure and Formalized Blockchain-IPFS Information Sharing in Precast Construction from the Whole Supply Chain Perspective, Ph. D. Candidate, School of Naval Architec- ture, Ocean and Civil Engineering, ShanghaiJiaoTongU- niv.,Shanghai200240,China.Email:dss514324152@sjtu.edu.cn,Professor, School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiao Tong Univ., Shanghai 200240, China (corresponding author).

[10] R. K. Marangappanavar and M. Kiran, "Inter-Planetary File System Enabled Blockchain Solution For Securing Healthcare Records," 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), Guwahati, India.