Blockchain Based File Storage System

Mrs. G. Sailaja[1], M. Srujana [2], A. SashyaSri [3], P. Shushrutha [4]
[1]Assistant Professor, Department of Cyber Security, Malla Reddy University, Hyderabad, Maisammaguda, Dulapally, Hyderabad-500100, Telangana, India
[2,3,4]Student/Research Scholar, Department of Cyber Security, Malla Reddy University, Hyderabad, Maisammaguda, Dulapally, Hyderabad-500100, Telangana, India

Abstract- This is a blockchain-based decentralized file storage application designed to ensure secure, immutable, and tamper-proof file management. Users can upload files of any type and size, which are stored in blockchain blocks alongside metadata such as the username, file size, and file data. The application employs a proof- of-work mechanism with a difficulty level of 3, utilizing a randomly generated nonce to validate and secure each block. Once a block is appended to the blockchain, it becomes immutable, preventing any unauthorized modifications or deletions. The decentralized architecture allows all peers to access and download stored files, eliminating reliance on a central authority while enhancing reliability and security. This innovative approach leverages blockchain's immutability and transparency to provide a robust solution for secure file storage and sharing, addressing challenges such as data integrity and unauthorized access.

Keywords- Blockchain, Decentralized File Storage, Proof-of-Work, Immutable Storage, Tamper-Proof File Management, Peer-to-Peer Network, Secure File Sharing, Data Integrity, Nonce-Based Validation, Cybersecurity, File Metadata, Secure Data Retrieval.

I. INTRODUCTION

In the digital era, data security, integrity, and availability are critical concerns for individuals and organizations. Traditional cloud storage solutions, such as Google Drive, Dropbox, and AWS S3, rely on centralized architectures, making them susceptible to data breaches, unauthorized access, and single points of failure. These vulnerabilities raise concerns about data privacy, reliability, and trust in third-party storage providers. As the demand for secure and decentralized file storage grows, blockchain technology has emerged as a viable solution due to its immutability, transparency, and distributed nature.

Blockchain-based decentralized storage eliminates the reliance on a single authority by distributing data across multiple nodes in a peer- to-peer network. This ensures that files remain secure, tamper-proof, and accessible even in the event of failures or cyberattacks. Existing decentralized storage solutions, such as the InterPlanetary File System (IPFS), Filecoin, and Storj, attempt to address these challenges; however, they often lack built-in security mechanisms or require paid services, limiting their accessibility.

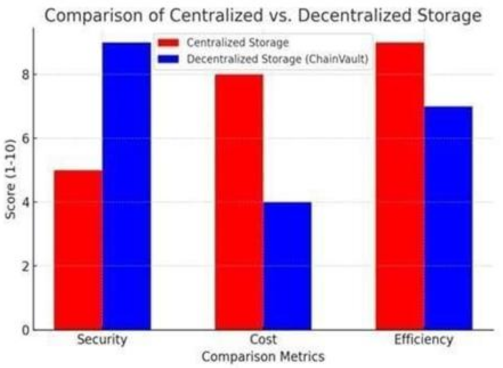
To overcome these limitations, It is proposed as a blockchain-based decentralized file storage system that enhances security, integrity, and accessibility. By integrating a proof-of-work (PoW) mechanism with a difficulty level of 3, it ensures computational effort is required for block validation, preventing unauthorized modifications. The system employs hashing techniques to maintain data integrity and leverages blockchain's immutability to provide a tamper-proof storage environment. Unlike traditional cloud storage, which depends on a central authority, allows users to upload and retrieve files securely from a decentralized network of peers.

This paper explores the design and implementation of file storage, detailing its system architecture, security features, and performance evaluation. The study highlights the advantages of decentralized file storage over conventional cloud-based solutions and discusses future enhancements to improve scalability and efficiency. By leveraging blockchain technology, provides a reliable, secure, and cost-effective alternative for decentralized file storage, ensuring data remains accessible, verifiable, and immutable.

II. LITERATURE SURVEY

Traditional file storage systems, such as Google Drive, Dropbox, and AWS S3, rely on centralized architectures that provide scalability and ease of access but suffer from significant security and privacy risks. These centralized solutions are vulnerable to data breaches, unauthorized access, and single points of failure. To address these challenges, decentralized storage solutions have been introduced, offering improved data security and resilience. One such system is the InterPlanetary File System (IPFS), which operates as a peer- to-peer content-addressable storage network. While IPFS enhances redundancy and efficiency, it lacks built-in security mechanisms such as proof-of-work, making it susceptible to unauthorized modifications.

Blockchain-based decentralized storage platforms like Storj, Filecoin, and Sia have attempted to provide a more secure alternative by leveraging cryptographic proofs and distributed ledger technology. These solutions ensure data immutability and enhance security; however, they often require users to pay for storage services and face network latency issues. While Filecoin introduces an incentive-based mechanism for data storage, it does not inherently prevent tampering without additional security layers. Similarly, Storj and Sia utilize encryption and decentralized distribution, but they still rely on external mechanisms for ensuring proof of data integrity.



It differentiates itself from these existing solutions by integrating a proof-of-work (PoW) mechanism with a difficulty level of 3, ensuring computational effort is required for block validation. This approach enhances the security and immutability of stored files while preventing malicious alterations. Additionally, ChainVault leverages blockchain's transparency and peer-to-peer accessibility to provide a decentralized, tamper-proof, and secure storage solution without incurring additional costs for users. Compared to traditional cloud storage, which remains vulnerable to unauthorized data manipulation, ChainVault offers a robust alternative that guarantees data integrity through hashing techniques and blockchain immutability. By addressing the limitations of existing decentralized storage systems, ChainVault presents an improved model that balances security, accessibility, and efficiency.

III. SYSTEM ANALYSIS

A. EXISITING SYSTEM

Traditional file storage systems rely on centralized cloud servers or data centers controlled by a single entity, making them vulnerable to various challenges. A major concern is the single point of failure—if the central server is compromised, all stored data is at risk. Additionally, centralized databases are frequent targets for cyberattacks, including data breaches and ransomware, posing significant security risks. Users also have limited transparency regarding how their data is managed, raising concerns about privacy and control. Furthermore, data integrity issues arise due to the potential for unauthorized modifications or deletions without user consent. While decentralized storage solutions like IPFS and Filecoin attempt to mitigate these challenges, they still face limitations in security and file verification.

B. PROPOSED SYSTEM

ChainVault is a secure, decentralized file storage and sharing solution. Users register and log in with hashed credentials, ensuring password security. Files are uploaded to Pinata (IPFS) with access control—senders grant read or read/write permissions to selected users. Each file upload and access involves gas fees, validated via MetaMask authentication. A unique hash is generated and emailed to authorized users; this hash is required for file access or modification. Storing metadata and using cryptographic verification ensures only authorized users can interact with files. ChainVault ensures confidentiality, integrity, and availability through decentralized storage and blockchain-based access control.

IV. METHODOLOGY

The methodology consists of multiple stages, including system design, implementation, and validation. This approach ensures a secure, decentralized, and efficient file storage and retrieval system using blockchain technology and a peer-to-peer (P2P) network. The following detailed steps outline the approach taken:

1. System Design

- Defining the System Architecture: Establishing a framework that enables secure file storage, retrieval, and access control while ensuring decentralization.
- Implementing Proof-of-Work (PoW) for Block Validation: A PoW mechanism is introduced to ensure that only valid transactions (file uploads and accesses) are recorded on the blockchain, preventing tampering or unauthorized modifications.

2. Blockchain Development

- Developing a Custom Blockchain Ledger: The blockchain stores file metadata, such as hash values, timestamps, and ownership information, ensuring a transparent and verifiable record.
- Implementing a Mining Algorithm with Difficulty Level 3: A mining process is used to validate new transactions, ensuring security and preventing unauthorized modifications.
  - Securing Transaction Processing for File Uploads and Access: Transactions related to file uploads, modifications.

3. Decentralized Storage & File Access

- Designing a Peer-to-Peer (P2P) Network: Files are not stored directly on the blockchain but are distributed across multiple storage nodes in a decentralized P2P network. This enhances scalability and efficiency.
- Implementing Secure File Retrieval Mechanisms: Users retrieve files using IPFS (Inter Planetary File System) or a similar decentralized storage protocol, ensuring efficient access.

4. Security Measures

- Applying Hashing Algorithms for Data Integrity: Each uploaded file is hashed using cryptographic hash functions to generate a unique fingerprint, preventing unauthorized modifications.
- Enforcing Immutability of Stored Files: Once a file is uploaded and its metadata recorded on the blockchain, it cannot be modified or deleted, ensuring a tamper-proof record.

5. Performance Evaluation

- Stress Testing for Scalability: The system is tested under high loads to determine how well it handles multiple concurrent file uploads, downloads, and blockchain transactions.
- Measuring File Retrieval Speed: The efficiency of file access from decentralized storage is evaluated to ensure low latency and optimal performance.

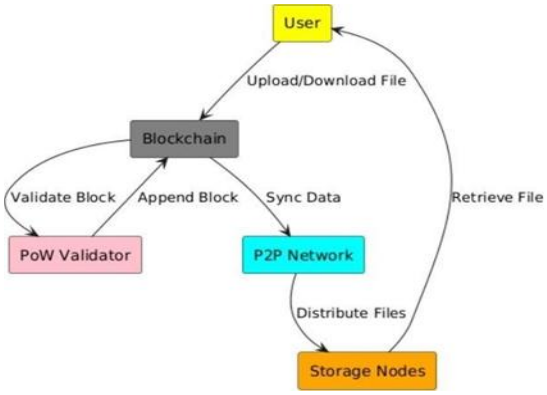
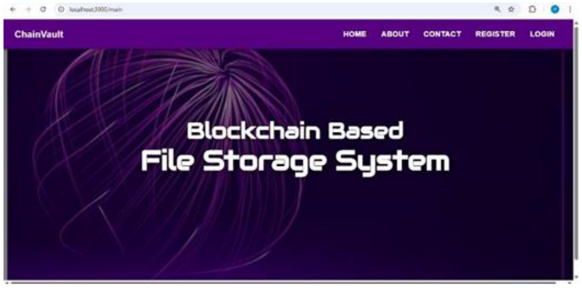


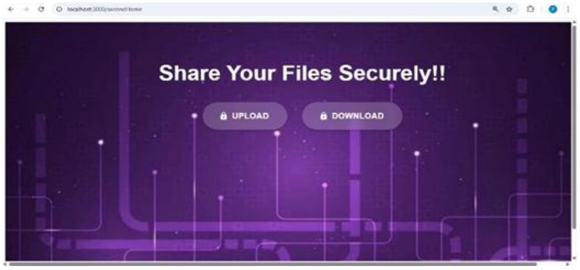
Fig : Architecture of a decentralized storage system using blockchain, PoW validation, and a P2P network.

V.RESULTS



Blockchain Based
File Storage System

Fig 1: The ChainVault web application running on localhost:3000 and the interface includes a centered welcome message and two authentication options—"LOGIN" and "REGISTER".



Share Your Files Securely!!

Fig 2: The File Sharing web application running on localhost:3000/secondHome and the interface includes a centered welcome message and two file management options—"UPLOAD" and "DOWNLOAD".

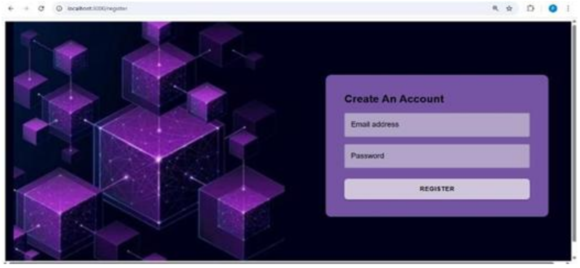


Fig 3: The user registration interface includes fields for Email and Password, along with a "REGISTER" button. A confirmation popup message at the top indicates successful user registration.

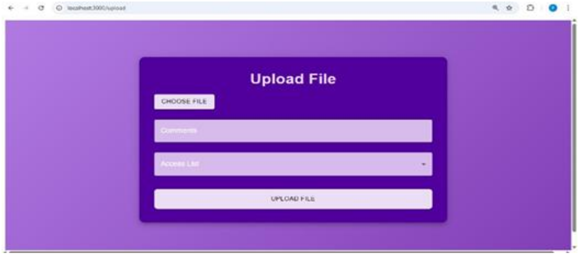
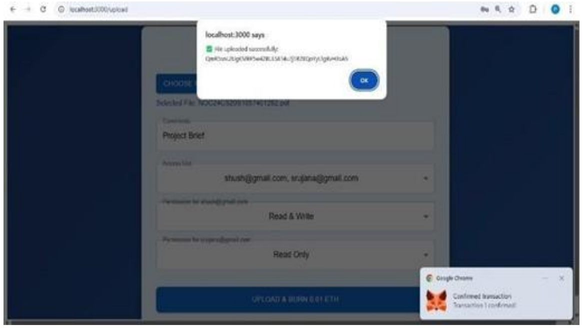


Fig 4: It allows user to select a file, add comments, specify an access list, and assign permissions. The "UPLOAD & BURN 0.01 ETH" button suggests blockchain-based file storage with Ethereum integration.



localhost:3000 says

✅ File uploaded successfully: QmR5uL2UgKMBF5w42BL35814u7j1B28QoYyLTgBvHXsAS

Selected File: NOC24CS2091057401282.pdf

Comments: Project Brief

Access List: shush@gmail.com, srujana@gmail.com

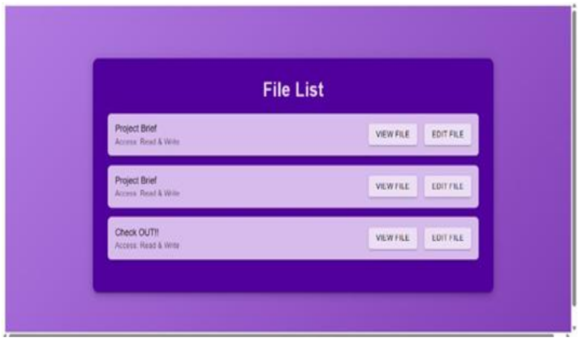
Permission for shush@gmail.com: Read & Write

Permission for srujana@gmail.com: Read Only

Confirmed transaction

Transaction 1 confirmed!

Fig 5: File has been successfully uploaded, with an IPFS hash displayed in a confirmation pop-up. A MetaMask notification at the bottom confirms a blockchain transaction related to the upload.

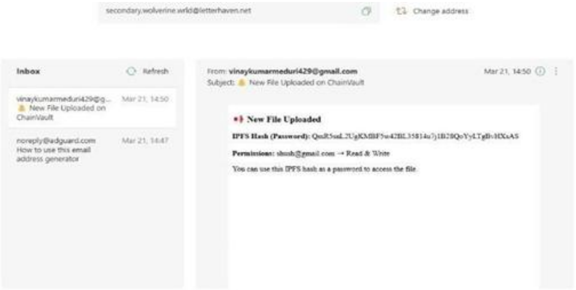


Project Brief
Access: Read & Write

Project Brief
Access: Read & Write

Check OUT!!
Access: Read & Write

Fig 6: This is the available file list.



secondary.wolverine.wrld@letterhaven.net

vinaykumarmeduri429@g... Mar 21, 14:50
New File Uploaded on ChainVault

noreply@adguard.com Mar 21, 14:47
How to use this email address generator

From: vinaykumarmeduri429@gmail.com Mar 21, 14:50
Subject: New File Uploaded on ChainVault

New File Uploaded

IPFS Hash (Password): QmR5uL2UgKMBF5w42BL35814u7j1B28QoYyLTgBvHXsAS

Permissions: shush@gmail.com → Read & Write

You can use this IPFS hash as a password to access the file.

Fig 7: email inbox displaying a notification about a new file uploaded on Chain Vault. The email contains an IPFS hash, which acts as a password to access the file, along with user permissions indicating "Read & Write" access for a specific email address.

VI. CONCLUSIONS

File storage system presents a blockchain-based decentralized file storage solution that ensures secure, immutable, and tamper-proof file management. By leveraging blockchain's cryptographic security and decentralization, the system eliminates the risks associated with centralized file storage, such as unauthorized access, data manipulation, and single points of failure. The implementation of a proof-of-work mechanism with nonce- based validation enhances the integrity and security of stored files, preventing unauthorized modifications or deletions. This approach effectively addresses critical challenges in data storage, such as security, integrity, and trust, making a robust alternative to traditional cloud storage solutions. Future improvements may involve optimizing proof-of-work efficiency and integrating advanced cryptographic techniques to further enhance security and performance.

V. FUTURE SCOPE

The future scope of this blockchain-based file storage and sharing system includes integrating advanced security protocols, AI-based threat detection, and decentralized identity management (DID). Enhanced security protocols, such as end- to-end encryption and multi-factor authentication, will protect files from unauthorized access. AI-powered threat detection can monitor system activity in real-time, identifying and preventing potential threats. Implementing DID will allow users to control their digital identities securely, enhancing privacy and reducing the risk of identity theft. These improvements will strengthen security, ensure faster threat response, and enhance access control, making the system more secure and efficient for future use.

REFERENCE

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] Wood, G. (2014). *Ethereum: A Secure Decentralized Generalized Transaction Ledger*. Ethereum Project Yellow Paper.

[3] Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*. Retrieved from https://arxiv.org/abs/1407.3561

[4] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *Blockchain Technology: Beyond Bitcoin*. Applied Innovation Review, 2, 6-19.

[5] Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. IEEE Security and Privacy Workshops, 180-184.

[6] Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). *Blockstack: A Global Naming and Storage System Secured by Blockchain*. USENIX Annual Technical Conference.

[7] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). *Securing Proof-of-Work Ledgers via Checkpointing*. ACM Transactions on Privacy and Security (TOPS), 21(1), 1-31.

[8] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). *Smart Contract-Based Access Control for the Internet of Things*. IEEE Internet of Things Journal, 6(2), 1594-1605.

[9] Mohanta, B. K., Panda, S. S., & Jena, D. (2020). *An Overview of Smart Contract and Use Cases in Blockchain Technology*. 2018 9th International Conference on Computing, Communication, and Networking Technologies (ICCCNT), 1-4.

[10] Wang, Q., Luo, X., Zhang, M., & Xu, Q. (2021). *A Secure and Efficient Blockchain-Based Cloud Storage Framework with Dynamic Data Auditing*. IEEE Transactions on Cloud Computing, 10(1), 69-81.