IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Decentralised Cloud Storage Using Blockchain Interplanetary file System (DApp)

Prof.A.M.Ingole , Harshal Bhangale , Vaishnavi Marne , Rutuja Raut

Department of Computer Engineering, BVCOEL Pune,India

Abstract-
This article proposes a cloud management system based on blockchain technology that uses a blockchain wallet for user authentication and integration with the Filecoin network. Users can securely store and share information by providing access control through smart contracts. This new system aims to address data security, privacy and availability in traditional cloud storage solutions. The design, process and details of the project are discussed and the optimization of the system is demonstrated. The study concludes by showing the consequences of the solution and its potential impact on the climate storage environment.

Key words: IPFS **(**Interplanetary File System),Smart contract

I. INTRODUCTION

The digital age has ushered in an unprecedentedera of data creation and use. The growth of data-driven applications, cloud computing, and the Internet of Things has created the need for secure, scalable, and accessible data storage solutions. Traditional cloud storage services play an important role in meetin g this need, but suffer from inability to deal with internal data management, user privacy and data accessi bility issues. Therefore, there is interest in using blockchain technology to create honest, reliable and se cure cloud storage. A new approach to cloud storage. In this system, users can securely store and share their data while controlling who can access their data. User authentication is done through a blockchain wallet, and smart contracts on the blockchain manage access. Combining the advan tages of Blockchain, Filecoin and user access control, this new solution aims to solve the fundamental pr oblems of data security and privacy in cloud storage.

II. LITERATURE REVIEW

The literature surrounding blockchain technology, decentralised storage solutions, and user authentication in the context of cloud storage is rich and varied. In this section, we provide an overview of relevant research, highlighting key findings, existing systems, and areas where this study contributes to the field.

[A] Blockchain Technology and Data Security:Blockchain technology has garnered considerable attention as a robust solution for data security and integrity. It is the backbone of various applications and systems that prioritise trust, transparency, and decentralisation.

Nakamoto's groundbreaking whitepaper introduced the concept of blockchain as a distributed ledger for Bitcoin, but its applicability extends far beyond cryptocurrency. Research has explored how blockchain technology can be harnessed to secure and authenticate data, offering a decentralised alternative to centralised databases. It offers immutability through its consensus mechanism, enabling trust in data stored on the blockchain.Moreover, smart contracts, self-executing code on the blockchain, have been instrumental in automating various processes. In cloud storage systems, they can be employed for access control, ensuring that only authorised users can access specific files.

Data on user authentication in the context of blockchain technology, trust solutions and cloud storage is rich. In this section, we provide an overview of related work, highlighting key findings, existing method s, and areas where this work contributes to the field. Blockchain technology has attracted much attention as a powerful solution for data security and integrity. It is the foundation of many practices and processes that improve trust, transparency and distribution. Its scope extends beyond cryptocurrencies. The research explores how blockchain technology can be used to protect and verify information by providin g an alternative to centralized storage. It provides immutability through the consensus mechanism, thus ensuring trust in the information stored in the blockchain. They can be used for administrative purposes in cloud storage systems to ensure that only authorized users can access certain information. U sing blockchain to ensure data security and smart contracts for management are key components of distrib uted cloud computing

[B] Decentralized storage solutions: The limitations of traditional centralized cloud storage solutions have spurred the development of decentralized alternatives. One of the most famous projects in this regard is Filecoin. Filecoin creates a global market for data storage by encouraging individuals and organizations to share unused storage. IPFS provides repeatability and usability by supporting data storage across mobile devices. The system plans to benefit from the efficiency and redundancy provide d by IPFS by integrating with Filecoin, while also taking advantage of Filecoin's business-oriented, Location based storage approach used to support storage space. User Authentication in Blockchain-based systems: User authentication is an important element in Blockchainbased systems. A blockchain wallet is an encrypted key that represents the user's identity on the blockchain and plays an important role in verifying the user's identity. The wallet is used to sign transactions that provide proof of ownership. Research shows that using blockchain wallets for authentication can increase security by eliminating traditional usernames and passwords that are vulnerable to data breaches. Recent research has explored consumer wallet applications, focusing on increasing the usability of blockchain applications.

blockchainbased authentication approach is essential toensure that users can easily interact with the share d cloud proposed in this study. Access control: Access control in decentralized cloud storage systems This is a huge area of research. Smart contracts are personal codes used on the blockchain and are used to verify access rights to stored information. These agreements may specify who can access, modify, or share information and under what circumstances. For example, Ethereumbased storage systems use smart contracts to manage access rights to data stored on the blockchain. The system plans to use a similar approach using smart contracts that allow users to control their data, decide who can access their data and what happens to it. The concept of controlling access to cloud storage systems has become an important aspect of data privacy and security. Traditional cloud storage services often control access centrally, giving users limited access to their data. This lack of control exposes users to privacy issues and data breaches.

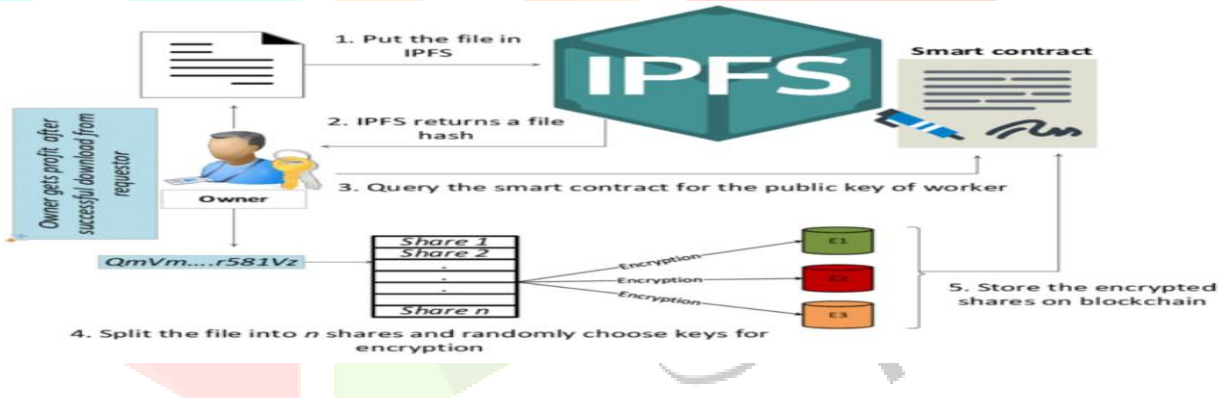
Users define who can access their data and dynamically manage permissions. The system plans to follow this shift to user management by empowering users to share access rights, increasing data privacy and security. The importance of blockchain technology in solving data security and access control issues, the emergence of decentralized storage solutions such as Filecoin, and usercentric user authentication and access to cloud storage management. The proposed decentralized cloud storage system combines elements to create a secure, user-controlled and problem solving solution. The next section of this article describes the design, process, and practical use of this in novation, as well as evaluating its effectiveness and potential impact in data storage and management. , forms the basis for discussing your cloud storage plan. You can expand on these topics by presenting unique research, discoveries, and advances in any field.

II. ARCHITECTURE

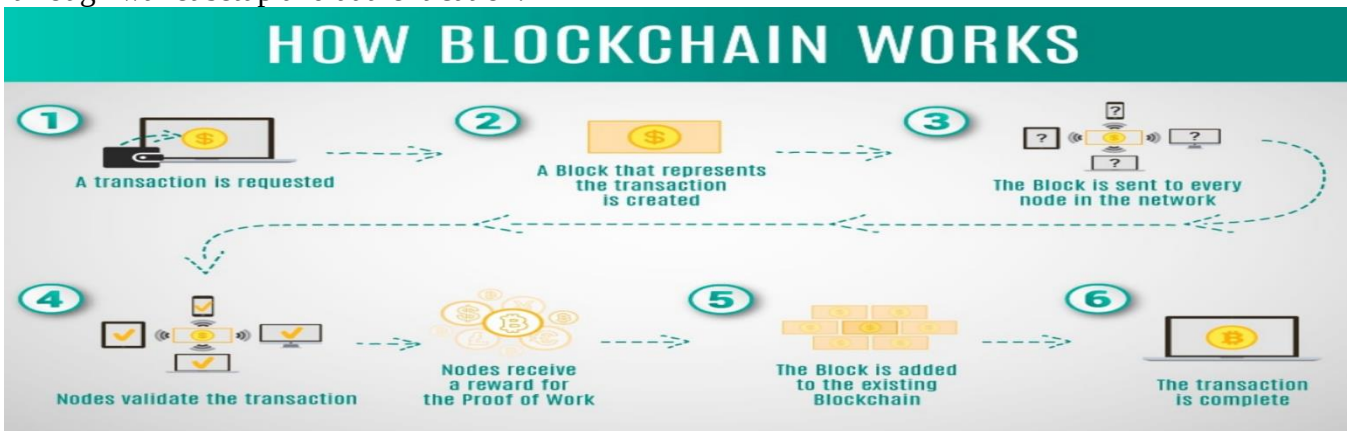
III.

The architecture of a decentralized cloud storage system represents the infrastructure that will provide security, usermanaged data storage, access control, and user authentication. This section provi des an overview of the main components and their interactions. A decentralized directory for user authe ntication and access control. Blockchain networks such as Ethereum were chosen for their security, consensus mechanisms, and smart contracts. These privacy agreements automatically govern rights and prior authorization by allowing or denying access to certain information. These wallets store the encryption keys required for user authentication. Users can sign transactions and access informatio n using a blockchain wallet that proves their identity. Users can store files securely on the IPFS network, and Filecoin works to encourage service providers to contribute their resources. This connection a llows users to upload, manage and share files, set access controls and authenticate using blockchain wal lets.

User registration and wallet: Users register in the system and create their own secure blockchain wallet . Wallet configuration creates a cryptographic key pair that is used for user authenticati on. These files are encrypted and then stored on the IPFS network, with their unique identifiers (CIDs) recorded on the blockchain. Smart contracts define the rules that govern access to this information. T he smart contract determines whether the user has the necessary permissions to access the data. If allowed , CID data will be retrieved from the blockchain and the user will be able to retrieve the data from the IP FS network. Smart contracts have been modified to reflect these changes, ensuring efficient and effe ctive access control. encryption. Data is encrypted before being uploaded to the IPFS network and the d ecryption key is stored on the blockchain and can only be accessed by authorized users. This encryption process, combined with the immutability and security of the blockchain, provides effective p rotection against unauthorized access and data leakage. The combination has many advantages. IPFS provides distributed and shared data storage, making data reproducible and accessible.



Filecoin's incentives encourage service providers to leverage their resources for reliability and efficiency. By using these technologies together, the system takes advantage of decentralized storage and business oriented solutions. Architecture that makes the system accessible to a wide range of users. It simplifies the process of uploading, managing and sharing data and is userfriendly even for those with blockchain restrictions. The user interface also improves the overall user experience by guiding users through wallet setup and authentication.



In summary, the architecture of the proposed decentralized cloud storage system aims to provide security , user control and efficient solutions for data storage. The system aims to solve information technology security, privacy and accessibility issues in cloud storage solutions by combining blockchain technology , smart contracts, Filecoin integration and user relationships. In the remainder of this article, the methods and techniques used in this architecture will be examined and their use and effectiveness will be demonstrated.

IV.METHODOLOGY

The methodology of this research paper describes the steps and methods taken to design, develop and imp lement a cloud storage management system. The process includes technology selection, smart contract creation, user authentication and access control procedures. There is also talk of integration with Filecoin and improving the user interface. Ethereum was chosen due to its mature ecosystem, smart contract capabilities and large user base. Other blockchain platforms have also been considered, but Ethereum's popularity and security features make it a tough choice. An lightweight user interface. Nodes form the backbone of the decentralized cloud storage system. These agreements specify who can access certain information and under what conditions. The management logic is built using Solidity, Ethereum's smart contract language. Smart contracts are designed to enforce these rules. Research and Integration Wallet: Blockchain Wallet: Guides users through the process of creating a blockchain wallet. The system generates a key pair for each user, providing them with a unique and secure user authentication process.

Authentication Workflow: Defines the user's authentication process. Users log in using the blockchain wallet by providing proof of their identity. This authentication process provides secure access to the system and related data. When users upload files, the files are encrypted and stored on the IPFS network. The corresponding identifier (CID) is stored on the blockchain for future retrieval.

Incentive mechanism: Filecoin's incentive mechanism is used to reward providers and encourage them to join the network. This system supports rewards for storage providers. It allows users to perform a variety of tasks, such as sending, managing and sharing information, setting up management systems and verifying blockchain wallets. Control strategy.

The system provides a usercentered approach to information sharing andaccess. or defects . Carefully examine the interaction between Blockchain, Filecoin and IPFS.

[G] User experience evaluation: User feedback: Real users participate in feedback on the user interface and system functionality. Their experiences and suggestions were recorded and evaluated for further development. The above information forms the basis of the development and implementation of decentralized cloud storage system. By following these steps, the research aims to create a secure, user-controlled and cloudbased solution that supports blockchain technology, Filecoin integration and a user-centric approach to data access and sharing. The rest of this article will describe the details of the project, evaluation results, and the impact of the cloud storage system.

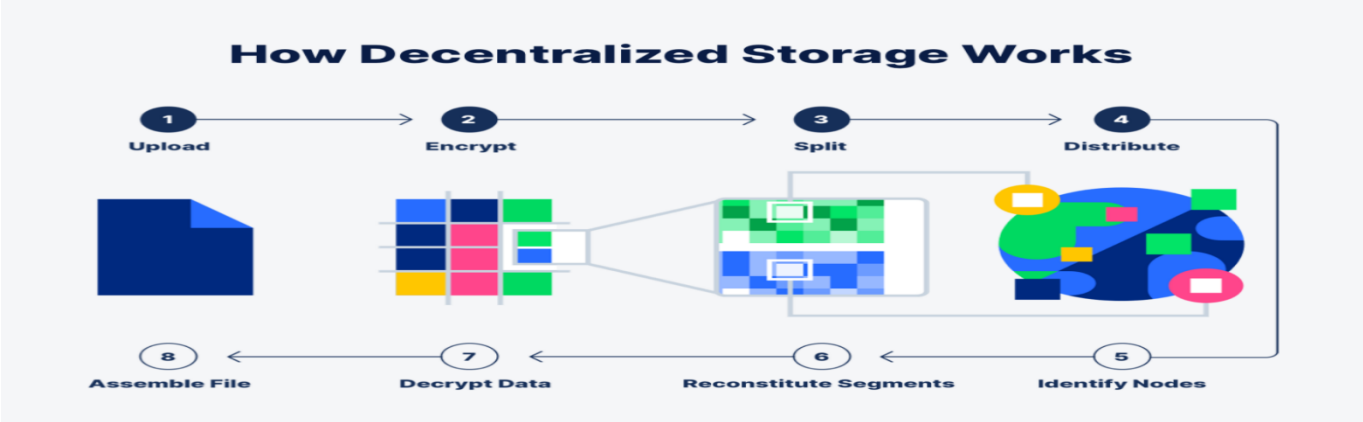
This chapter provides an overview of the implementation and implementation of decentralize d cloud storage systems. It involves various skills, user interaction and system operation. size node. Nodes work together to ensure the reliability and security of the system.

Smart Contract: Access Control Smart Contract: Smart contracts are designed to control access to share d data. These contracts are written in Solidity and sent to the blockchain network for rules to be enforced. The wallet creation process creates a encryption pair for user authentication. Points needed to build their wallets. These files placed in the system were previously encrypted and stored in the IPFS network. The relevant CID is recorded in the blockchain. Authentication: Users log into a blockchain wallet by providin g cryptographic credentials on their own. The smart contract determines whether the user has the necess ary permissions to access the data. Functionality: The system allows users to collaborate and share infor mation in accordance with a team environment. and availability. The CIDs of these files are recorded on the blockchain, making them retrievable.]

User-friendly user interface: The user interface is designed with a user-centered approach and is quite friendly for users from different backgrounds. :

Detailed access control: Users can easily manage access control rights to their data through the user inter

face that supports granular control. System components, including smart contracts, encryption systems, and user authentication systems, are rigorously tested to identify and fix vulnerabilities. This step ensu res that the interaction between blockchain, Filecoin, and IPFS works smoothly. . Suggestions written by users help improve and improve the system interface and functionality. br>Blockchain Security: Us e appropriate security measures to protect users' blockchain wallets and private keys from unauthorized access. The system is designed to be scalable, allowing for increased user interaction as the user base expands and data capabilities grow. Chain and decentralized storage technology. Measures taken.



V. PROJECT DETAILS

This section provides a comprehensive overview of the practical implementation and execution of the proposed decentralised cloud storage system. It encompasses various technical aspects, user interactions, and the system's real-world functionality.

[A]Technical Implementation:System Setup:Blockchain Node Configuration: Multiple nodes are set up to form the blockchain network, including full nodes and lightweight nodes. These nodes work in tandem to ensure the reliability and security of the system.

Smart Contracts:Access Control Smart Contracts: Smart contracts are developed to manage access control for shared files. These contracts are written in Solidity and deployed on the blockchain network to enforce predefined rules.

Wallet Integration:Blockchain Wallet Creation: Users can create blockchain wallets through the system's interface. The wallet creation process generates cryptographic key pairs used for user authentication.

[B] User Interaction:

Registration and Authentication:

User Registration: Users can register with the system, providing necessary details to create their accounts.Wallet Setup: During the registration process, users are guided through wallet setup, including securing their private keys.

File Management:

File Upload: Users can upload files to the system, which are encrypted before being stored on the IPFS network. The **relevant** CID is recorded **in** the blockchain.Access Control Configuration: Users can specify access control policies, allowing them to define who can access, modify, or share their files.

Authentication and Access:

User Authentication: Users log in using their blockchain wallets, providing cryptographic proof of their identity.

Access requests: When a user requests access to data, the blockchain verifies the request. The smart contr act determines whether the user has the necessary permissions to access the data.

Sharing and Collaboration:

File Sharing: Users can share files with other users, with the flexibility to configure access control policies based on their preferences.

Collaborative Work: The system enables users to collaborate on shared files, making it suitable for team environments.

[C] Filecoin Integration:

Storage Mechanism:

File Storage on IPFS: Files uploaded by users are stored on the IPFS network, ensuring redundancy and accessibility. The CIDs of these files are recorded on the blockchain, making them retrievable.
Incentivization:
Filecoin Rewards: The system integrates Filecoin's incentivization mechanism, rewarding storage providers for contributing their resources to the network.
[D] User Interface
User-Centric Design:
User-Friendly UI: The user interface is designed with a user-centric approach, making it intuitive for users of varying technical backgrounds.
Access Control Management:
Granular Access Control: Users can easily manage access control policies for their files through the user interface, promoting fine-grained control.
[E] Testing and Evaluation
Quality Assurance:
Unit Testing: All system components, including smart contracts, encryption mechanisms, and user authentication processes, undergo rigorous unit testing to identify and rectify vulnerabilities.
Integration Testing: The system components are thoroughly tested for proper integration and data flow. This step ensures that the interaction between blockchain, Filecoin, and IPFS functions seamlessly.
Performance Evaluation: The performance of the system is benchmarked for various parameters, including file upload and retrieval times, transaction processing speeds, and access control verification times.
User Experience Assessment:
User Feedback and Usability Testing: Real users participate in usability testing and provide valuable feedback regarding their experiences. The feedback collected from users helps in refining and enhancing the system's interface and functionality.
[F] Security Measures Data Encryption: The encryption of files ensures that data remains confidential and secure throughout the storage and access processes.
Blockchain Security: Appropriate security measures are implemented to protect users' blockchain wallets and private keys from unauthorised access.
[G] Scalability and Future Enhancements
Scalability: The system is designed to be scalable, allowing for increased user participation and file storage capacity as the user base expands.
Future Developments: Ongoing development and enhancements are planned, with a focus on improving user experience, enhancing access control options, and exploring additional blockchain and decentralised storage technologies.

VI.Conclusion

In summary, our research shows the criminal landscape that leads to the use of blockchain technology integrated with Filecoin, which is important for user control access. The use of the technology demonstrates its ability to transform cloud storage by improving data security, user privacy, and ease of access. As the digital environment continues to evolve, security solutions for consumer applications like these become vital. The journey to data security, privacy, and user empowerment has just begun, and this research is an important step .

VII. ACKNOWLEDGEMENT

Prof. J.S. We thank our guide Mahajan and our department for their support, guidance and assistance during the research of the survey.Their wisdom, encouragement and guidance are crucial in the development of our journey.
We are grateful to them for their commitment to our success. Thank you for being a pillar of knowledge and support and for the important role you play in our success.

VIII. REFERENCES

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

[2]. Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. Retrieved from https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[3]. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

[4]. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

[5]. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Retrieved from https://ethereum.github.io/yellowpaper/paper.pdf

[6]. Protocol Labs. (n.d.). Filecoin: A Decentralised Storage Network. Retrieved from https://filecoin.io/filecoin.pdf

[7]. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.

[8]. Gupta, P., & Garg, R. (2019). Secure Data Sharing in Ethereum: An Access Control Scheme for Decentralised Applications. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (pp. 618-623). IEEE.

[9]. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralised digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

[10]. Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.