WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Based File Sharing System

Prof. Mr. M. Velludurai[1], Rahul Gond[2], Omkar Acharekar[3], Snehal Sanap[4], Anushka Nipurte[5]

[1]Dept. of Information Technology Engineering, Armiet, Maharashtra, India
[2]Dept. of Information Technology Engineering, Armiet, Maharashtra, India
[3]Dept. of Information Technology Engineering, Armiet, Maharashtra, India
[4]Dept. of Information Technology Engineering, Armiet, Maharashtra, India
[5]Dept. of Information Technology Engineering, Armiet, Maharashtra, India

ABSTRACT

Cloud storage is one of the leading options where you can keep big data, however, a way to keep a single cloud space using a computer is not secure. On the other hand, Blockchain is a cloud-based storage system that ensures data security. Any computer node connected to the Internet can join and build peer networks thus increasing utilization of resources. Blockchain is a peer-to-peer system distributed per node on the network that keeps a copy of the blockchain thus making it invariant. In the proposed system, the user file is encrypted and stored on multiple peers in the network using IPFS (Inter Planetary File System) protocol. IPFS creates hash values. The hash value indicates the path of the file and is stored in the blockchain. In this project we use the blockchain and ipfs cloud platform for storing the file of n users. Once the user uploads any file it will get encrypted and that file stored on ipfs and file metadata will be stored on blockchain. And at the time of downloading the particular file, the metadata of that file will be retrieved from the blockchain and the file will be decrypted and displayed to you. Smart contracts are used to store file details in the blockchain and also transfer the cryptocurrency (ETH) from the user's wallet to the peer's wallet. AES encryption algorithm for enhancing the security of user's data stored in cloud storage. This paper focuses on secure data shared across the country storage, high availability of data, and efficient use of storage facilities.

Keywords: A possible keyword using the blockchain-based file sharing system could be "decentralized file sharing." This refers to the use of a blockchain network to facilitate peer-to-peer file sharing, without the need for a central authority or intermediary. Another related keyword could be "immutable file sharing," as the use of blockchain technology allows for secure and tamper-proof sharing of files, which cannot be altered or deleted once added to the blockchain.

INTRODUCTION

The first description of blockchain technology appeared in 2008 in the article Bitcoin: a peer-to-peer payment system, an electronic cash system described as a record of Bitcoin transaction history. a structure that sequentially combines blocks of data in chronological order. A cryptographic procedure is used to ensure that the distributed ledger cannot be damaged or manipulated. In general, blockchain technology uses the blockchain's data structure to verify and store data, uses distributed nodes and consensus algorithms to generate and update data, and uses cryptography to ensure the security of data transmission and access protect. A new distributed infrastructure and computing paradigm for programming and manipulating data using smart contracts consisting of automated script code. Blockchain has the following characteristics Distributed architecture. Blockchain is based on a distributed peer-to-peer network where all transactions are recorded. in "hybrid ledgers" at each network node, not in a normal server or data centre. Al

nodes update the ledger synchronously, reflecting the characteristics of decentralisation. reliable data source Mathematical principles and procedural methods make the whole system open and transparent, and there is no need for a trusted third party to reach consensus. Anyone can join the blockchain, and the blockchain is transparent and open to anyone with internet access.

At the same time, users can see that every transaction recorded in the superblock has not been tampered with. Blockchain uses string data structures with a specific SHA256 value and timestamp for each block, which have strong traceability and verifiability. At the same time, the cryptographic algorithm and consensus mechanism prevent manipulation of an indeterminate blockchain. Blockchain, in general, is a new type of distributed computing architecture based on cryptography, peer-to-peer network communication, a consensus algorithm, smart contracts, etc. cloud upload of job scheduling information.

OBJECTIVES OF THE PROJECT

- Identify and develop an effective strategy for a secure technology platform.
- Review and critically examine available theory, research, and practical citations, leading to fruitful conclusions.

- Investigate pertinent questions about the effectiveness of secure transactions using blockchain technology, with a particular focus on security and immutability.
- Develop a conceptual or theoretical framework for secure and efficient transaction entry using blockchain technology.
- Identify the key attributes that contribute to the effectiveness of secure transactions input using blockchain technology.

Benefits of Blockchain Based File Sharing Sysytem

A blockchain-based file sharing system offers several benefits over traditional file sharing systems. Here are some of the main benefits:

Security: The blockchain is a secure and decentralized system that uses cryptography to protect data. This makes it nearly impossible for anyone to tamper with the data or steal it. As a result, blockchain-based file sharing systems are more secure than traditional file sharing systems.

Decentralization: Blockchain-based file sharing systems are decentralized, meaning that there is no central authority controlling the system. This makes the system more resilient to attacks and ensures that there is no single point of failure.

Transparency: The blockchain is a transparent system that allows anyone to see the transactions that have taken place on the network. This makes it easier to track the history of a file and ensures that all users have access to the same information.

Cost-effective: Blockchain-based file sharing systems can be more cost-effective than traditional file sharing systems because they eliminate the need for intermediaries. This means that users can save money on transaction fees and other costs associated with traditional file sharing systems.

Immutable: Once a file is uploaded to a blockchain-based file sharing system, it cannot be deleted or modified. This ensures that the data remains secure and unaltered, providing a tamper-proof record of the file's history.

Overall, a blockchain-based file sharing system offers a secure, decentralized, transparent, and cost-effective way to share files. It is particularly useful for sensitive or confidential data that requires a high level of security and protection from unauthorized access or modification.

EXISTING SYSTEM:

- Blockchain networks can be used for two purposes. The integrity of the hash data collected from cloud collection to the block chain network is protected and stored in a distributed manner to ensure stability. In addition, each response from the cloud server and website access will be recorded in a block series for further review or investigation. Not only will the data record be kept permanently, but also, a data block will be generated to validate the data. The cloud server processes data from cloud collections and data access records, which are the same function as block chain networks.

- To secure the data record, the cloud server is obliged to request block data from the block chain network as permanent proof of data integrity. Additionally, data analytics data analysis and control system and server analysis can help determine the first stage of denying a distribution of service attacks. block chain network data and block production. Cloud data validation, auditing and decision making. The main steps are as follows: Business ID registration. In this program, we first register the ID number of each business in the cloud collection to identify collected data.
- After registering, start collecting data, which is the log file generated to schedule cloud work in the collection. We treat each log as an object and speed up individual data to improve efficiency before uploading to a block chain network. Raw data is also stored on a cloud website for future reference. Data transfer and commands.
- Each data collected from the cloud collection is structured as a meta-ancestor time data. After sending a meta-ancestor to the control system, the control system transfers hash data to the block chain network and sends the original data to the cloud database. At the same time, the control system will revert back to the cloud collection of some command data, these commands will also be converted to time, command format, recorded in the block chain.

FUTURE SCOPE:

Blockchain-based file sharing system can be extensive and involve various aspects of development, implementation, and maintenance. Here are some potential areas that might be included:

- System Design: Defining the system architecture, selecting the appropriate blockchain platform, developing protocols for file sharing and access control, and determining the data storage and retrieval mechanisms.
- Smart Contract Development: Creating smart contracts to automate the file sharing process, define access control policies, and ensure the integrity and security of data shared on the system.
- User Interface Development: Designing a user-friendly interface that allows users to upload, share, and manage files securely and efficiently.
- Blockchain Integration: Developing the necessary integrations between the file sharing system and the blockchain platform, including setting up nodes and ensuring secure communication between the two.
- Security and Privacy: Ensuring the system is secure against unauthorized access, implementing encryption for data in transit and at rest, and maintaining user privacy.
- Testing and Deployment: Conducting rigorous testing to ensure the system works as intended and is reliable, and deploying the system in a production environment.

FUTURE MODIFICATION

In the future, a flexible editing algorithm could compile files that can be accessed multiple times per user compared to the rarely accessible. This will help ensure that accessible files are always readily available to the user whenever needed. Also, credit the program can be added to each of its assigned peers 100 credit default, based on the operating time of their system, and a few Successfully granted file access requesting that their credits receive you drawn or added. Peer-to-peer peers will be given the most important thing to keep data.

PROPOSED SYSTEM

The user first creates an account on the metamask. The user's account address and wallet balance are fetched in the app through web3.js from the metamask. Users select the file to upload through file picker. System checks for the number of available peers. Further, the AES algorithm uses the user's wallet address as a key and encrypts the uploaded file. A payment dialogue seeks for the user's confirmation. On confirming the payment, the user's file is stored across available peers using IPFS protocol. IPFS then returns a hash value consisting of the path of the file. This path is then mapped with the user's address using a smart contract and gets stored securely in the blockchain. To achieve high availability and reliability of data, the uploaded data is replicated on three peers. For better performance the system blacklists peers every time they are unavailable for data retrieval. The terminology is briefly discussed below.

- Metamask : Browser extension which acts as a bridge to connect with the ethereum network.
- Ethereum Network : It is an open-source, public blockchain- based distributed computing platform. Ethereum uses smart contracts where one can add business logic to make decentralized applications as per the business requirements. Peers: These are the users of the system who have pledged to rent their free storage for an other user's to store files.
- AES: Advanced Encryption Standard (AES) is a symmetric- key algorithm that supports block length of 128 bit and can have a key size of 128, 192, and 256 bits.

- IPFS protocol: IPFS is an open-source peer to peer file transfer protocol.

ADVANTAGES OF THE PROPOSED SYSTEM

1. A hybrid cloud gives businesses the flexibility to adopt the most appropriate and innovative solution for the organization and choose from a range of management and service models from multiple vendors, preventing vendor lock-in.
2. Many organizations have moved to the hybrid cloud for greater scalability. A hybrid cloud environment allows organizations to scale resources and optimize performance based on the organization's changing needs.
3. Time-to-market can be the defining factor in an organization's competitive edge. The hybrid cloud helps organizations optimize IT performance to speed up the time to deliver products and services to customers.
4. In this digital era, businesses need the ability to adapt and change direction quickly. Using the hybrid cloud model, organizations can connect existing technology and on-prem infrastructure to cloud resources for added agility.

CONCLUSION

The proposed system improves data security by encoding and disseminating data to multiple peers in the system. The operating system uses the AES 256 bit encryption algorithm to encrypt data that ensures the confidentiality of user data. The encrypted data is then transmitted and stored to peers on the network using the IPFS protocol. Our system not only solves the privacy and security of central cloud storage but also provides peers to rent their unused storage and receive cryptocurrency returns, thus maximizing the use of the storage facility.

The proposed system improves data security by encoding and disseminating data to multiple peers in the system. The operating system uses the AES 256 bit encryption algorithm to encrypt data that ensures the confidentiality of user data. The encrypted data is then transmitted and stored to peers on the network using the IPFS protocol. Our system not only solves the privacy and security of central cloud storage but also provides peers to rent their unused storage and receive cryptocurrency returns, thus maximizing the use of the storage facility.

REFERENCE

A. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.--URL: https://bitcoin.org/bitcoin.pdf (2008).

B. Cachin, C., & Vukolic, M. (2017). Blockchain consensus protocols in the wild. Proceedings of the 31st International Symposium on Distributed Computing (DISC'17), 1-15

C. Dey, S., & Mukhopadhyay, D. (2019). A blockchain-based decentralized storage system for secure sharing of IoT data. International Journal of Distributed Sensor Networks, 15(5), 1550147719845955.

D. .Li, S., Li, C., Cao, Y., Li, X., & Jiang, S. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. In IEEE International Congress on Big Data (pp. 557-564). IEEE.

E. Shafagh, Hossein, et al. "Towards blockchain-based auditable storage and sharing of IoT data." Proceedings of the 2017 on Cloud Computing Security Workshop. 2017.

F. Zhu, Y., & Yao, Y. (2021). Blockchain-based cloud storage: A survey. IEEE Communications Surveys & Tutorials, 23(3), 2346-2373. Jiang, H., Shen, J., & Ma, J. (2021).

G. Blockchain-based secure and efficientdata storage in smart cities. Journal of Ambient Intelligence and Humanized Computing, 12(8), 8349-8363

H. Li, C., Li, J., Chen, L., & Chen, G. (2021). A review of blockchain-based secure data storage and sharing in healthcare. Journal of Medical Systems, 45(2),19.

I. (2016). On scaling decentralized blockchains. In Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research, 106-125.

J. Buterin, V. (2014). A next-generation smart contract and decentralized application platform Ethereum white paper, 1-32.

K. Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymousdistributed E- cash from Bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13), 397-411.

L. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technologybehind bitcoin is changing money, business, and the world. Penguin.

M. Zohrevandi, B., Habibi Lashkari, A., & Kazemi, H. (2020). Blockchain-based secure data storage and sharing in smart cities: Challenges, opportunities, and solutions. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5023-5043.

N. Dey, S., & Mukhopadhyay, D. (2019). A blockchain-based decentralized storage system for secure sharing of IoT data. International Journal of Distributed Sensor Networks, 15(5), 1550147719845955.

O. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.--URL: https://bitcoin.org/bitcoin.pdf (2008).

P. Cachin, C., & Vukolic, M. (2017). Blockchain consensus protocols in the wild. Proceedings of the 31st International Symposium on Distributed Computing (DISC'17), 1-15