INTER-ORGANIZATIONALFILESHARINGUSINGBLOCKCHAIN

Suresh Reddy Komsani
Lecturer in Computer Science
Governmnet Degree College,Yellareddy Dist: Kamareddy

Abstract

A consortium of organizations collaborates and exchanges information to create synergies in their operations. Centralized systems of secure transferring of data cannot provide distributed trust and transparency. Block chain technology can be used to transfer data securely and transparently. This paper proposes a block chain based secure transferring of data. It can be used by a consortium of organizations to securely exchange files in a distributed fashion. Hyper ledger Fabric, an enterprise block chain framework, is used for block chain network setup and the development of smart contracts. The Inter Planetary File System (IPFS) is used for storing files in a distributed way. The paper provides the workflow for identity management and file-sharing processes. The proposed system allows a consortium of organizations to share files with confidentiality, integrity, and availability using block chain. To meet the increasing demand for secure and efficient data sharing within logistics networks, we propose a decentralized Hierarchical Attribute-Based Encryption (HABE) scheme integrated with block chain and edge computing. Our solution introduces a privacy-preserving encryption strategy that allows edge devices to securely transmit data to nearby cloud nodes for processing. Additionally, a block chain-based data-sharing framework is developed, utilizing both edge and cloud storage to ensure decentralized access control. The system incorporates a Secure Hash Algorithm (SHA) to enhance authentication, enabling reliable and tamper-resistant verification of user access rights at the network edge. By combining HABE, block chain, and SHA, the proposed architecture ensures strong privacy protection, secure data sharing, and improved authentication efficiency.

Keywords: Block Chain Technology, IPFS, File-Sharing, Organizations Collaborates, Secure And Efficient Data Sharing

INTRODUCTION

This Study presents "Secure Cloud File Sharing System," a revolutionary cloud file sharing system that addresses these pressing concerns by harnessing the transformative power of block chain technology. Secure Cloud File Sharing System leverages the Ethereum block chain's distributed ledger technology, ensuring a tamper-proof and transparent record of all file-sharing activities. This distributed ledger system replicates data across a network of computers, eliminating the risk of a single point of failure and enhancing system reliability. In the event of a cyber-attack or hardware failure on one node, the data remains secure and accessible on the remaining nodes within the network. Additionally, the immutability of the block chain ensures that past records cannot be tampered with, fostering trust and transparency within the data sharing ecosystem. Secure Cloud File Sharing System integrates the Inter Planetary File System (IPFS) for distributed file storage, promoting data redundancy and availability. IPFS departs from the traditional client-server architecture, instead employing a peer-to-peer network for data storage. This distributed approach ensures that uploaded files are replicated across multiple devices within the network, enhancing data resilience and accessibility. Even if a node storing a particular file becomes unavailable, the file remains accessible through other nodes within the network. This redundancy safeguards against data loss and outages, ensuring that authorized users can consistently access their files. The subsequent sections of this paper delve deeper into the architecture and functionalities of Secure Cloud File Sharing System. We will explore the system's design principles, underlying technologies (Ethereum block chain, IPFS, smart contracts), and the step-by-step process of file upload and retrieval. Furthermore, the paper will discuss the security advantages offered by Secure Cloud File Sharing System compared to traditional cloud storage solutions. Finally, we will conclude by highlighting the potential applications and future directions for this innovative file sharing system. To deal with those obstacles, decentralized technology which include block chain and Inter Planetary File System (IPFS) have received reputation in latest years. Block chain, initially evolved for virtual currencies which include Bit coin, is an allotted ledger era that permits stable and obvious transactions without the want for vital intermediaries. IPFS, on the opposite hand, is a peer-to-peer document machine that offers a

decentralized and content-addressed garage version. Together, block chain and IPFS have the capacity to offer stable and green document garage and sharing answers without the want for vital intermediaries or third-celebration services. In the realm of digital information management, traditional centralized cloud storage systems face escalating concerns over security vulnerabilities and a susceptibility to breaches. While cloud storage remains a primary option for handling extensive datasets, the drawbacks of centralized control have prompted a paradigm shift. Block chain technology has emerged as a transformative force, introducing decentralized file sharing and storage systems that fundamentally alter the landscape of data management. The essence of this shift lies in moving away from centralized models, where data resides in single points of control, towards a decentralized framework facilitated by block chain.

LITERATURE REVIEW

Dr. Neeta P. Patil (2025) With the growing demand for secure, decentralized file sharing solutions, this study presents a block chain and IPFS-based framework for efficient data storage and access control. The proposed system leverages asymmetric encryption, smart contracts, and distributed access management to ensure confidentiality and integrity. The files are encrypted using AES-256 before they are stored in IPFS, and SHA-256 hashing is used to verify the content. Access control is guaranteed using block chain-based policies, encrypting access keys and dynamic permissions to ensure that users can exchange files. An intelligent contract automates authentication, access and distribution of keys, minimizing dependence on centralized bodies. In addition, suppliers of storage facilities for an incentive mechanism reward the economy of economic and scalable storage. By using consensus mechanisms, such as proof of aspiration (POS) or proof of the authorities (POA), the system prevents unauthorized modifications and increases data security. This approach provides a reliable solution for organizations requiring controlled access to confidential data, with potential applications in the field of financial, health care and public sectors.

Wanzong Peng (2024) File sharing, being the foundation of the Internet, has traditionally relied on a centralized service architecture resulting in significant maintenance costs. Moreover, due to the lack of an effective file management system, instances of sensitive information going out of control and loss of confidentiality in file sharing have occurred frequently. In order to address the difficulty of tamper detection and the lack of supervision in the entire process of file transfer in the current Internet environment, this paper designs a block chain-based system architecture for secure sharing of electronic documents. An efficient block chain model is used in our framework, and with the help of distributed storage system and asymmetric encryption technology, file sharing can be controlled, reliable and traceable in the transfer process. Referring to existing consensus mechanisms, e.g., Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT), we propose a new consensus for efficient and secure file sharing. Our experimental results show that our framework can maintain a higher throughput than existing schemes.

Niraj Wadile (2023) Cloud storage is one of the leading options to store massive data, however, the centralized storage approach of cloud computing is not secure. On the other hand, Block chain is a decentralized cloud storage system that ensures data security. Any computing node connected to the internet can join and form peers network thereby maximizing resource utilization. Block chain is a distributed peer-to-peer system where each node in the network stores a copy of the block chain thus making it immutable. This paper focuses on decentralized secure data storage, high availability of data, and efficient utilization of storage resources. When you add a file to IPFS, your file is split into smaller chunks, cryptographically hashed, and given a unique fingerprint called a content identifier. This CID acts as a permanent record of your file as it exists at that point in time. When other nodes look up your file, they ask their peer nodes who are storing the content referenced by the file's CID. When they view or download your file, they cache a copy and become another provider of your content until their cache is cleared. IPFS uses content addressing to identify content by what's in it rather than by where it's located. Looking for an item by content is something you already do all the time.

Peng Kang (2022) Under the current national network environment, anyone can participate in publishing. As an important information resource, knowledge files reflect the workload of publishers. Moreover, high-quality knowledge files can promote the progress of society. However, pirated inferior files have the opposite effect. At present, most organizations use

centralized servers to centrally manage the knowledge files released by users. In addition, it is necessary to introduce an untrusted third party to examine and encrypt the contents of files, which leads to an opaque process of file storage transactions, tampering with intellectual copyright, and the inability to have consistent systems of file management among institutions due to the lack of uniform standards for the same intellectual files. The purpose of this paper is to ensure the safe storage of knowledge files on the one hand and to realize efficient sharing of copyrighted files on the other hand. Therefore, this paper combines NDN (Named Data Network) technology with a distributed block chain and an Interplanetary File System (IPFS) and proposes a block chain knowledge file storage and sharing method based on an NDN. The method uses the NDN itself for the file content signature and encryption, thereby separating the file security and transmission process.

Devesh Solanki (2021) The widespread adoption of smartphones has replaced desktop computers and laptops as the first component of the computer, due to mobility, regular communication and application versatility. Mobile devices include extensive data storage including sensitive objects such as verification credentials, photos, videos, personal information, activity details, and much more. Therefore, protecting data stored on mobile devices becomes a serious problem. In this update, we are investigating the safety of the Android storage model between 2013 and 2018. Several threats are found in literature that can be classified as physical or software threats. Interest in the block chain has hit the top levels recently. While most of the buzz has been around for block chain use like crypto currencies and ICOs, the technology itself is exciting. The block chain provides democratized trust and authentication protocols that have already disrupted banking and are at risk of adding health care, financial services, social apps and more We use Block Chain and IPFS to store Hash values and files, secure file transfers can also be obtained.

Block chain-based storage system

Through a decentralized network, block chain system assures the safety and integrity of data storage and exchange across a wide range of applications. In respect of block chain-enabled technologies, found that data sharing and storing rank second only to IoT technology in terms of popularity. This research covers many fields, including tamper-proof mechanisms, encrypted storage, and block chain systems. Building reliable block chain systems for data sharing is a recent research hotspot. There are restrictions on how block chain data is stored. According to the block chain adopts a decentralized mechanism, and the ledger data is saved at all nodes at the same time. In this way, the data is almost never lost, and the nodes can restrict each other to prevent malicious tampering. However, it will generate a large amount of redundant information and seriously reduce the efficiency of the transaction.

Decentralized Cloud Storage Using Block chain

Introduces a methodology that uses Block chain applications to interact either directly with block chains or with smart contracts in order to achieve consensus on transactions, data or execution. A network of heterogeneous nodes stores the block chain, processes transactions and, if necessary, executes smart contracts. This leads to the following issue when working with large data files. Because the files are usually not required for the block chain nodes to function, the block chain becomes bloated, resulting in data being replicated on a large number of nodes data is analyzed. The block chain contains a series of transactions organized logically inside a block, these blocks are tied together using encryption in order to form a chain. The technology itself forms a decentralized consensus allowing peers to reach consensus on the state of a transaction.

Integrating Block chain And The Interplanetary File System

This Study introduces integrating block chain and Interplanetary File System (IPFS), hence understanding what the terminologies mean is mandatory. Block chain is a decentralized database that keeps a permanent record of information and stores it in blocks in consecutive, cryptographic patterns linking these blocks to form a chain. It almost nullifies the chances of hacking the database due to the cryptographic encryption technique used in the block chain. The digital ledger transaction is duplicated and spread across various nodes of the computer which makes it transparent, decentralized, and immune to

tampering network. Since block chain cannot store large files due to size limitations and high cost, an alternative is necessary to store large files and get the benefits of the decentralized database. This can be achieved with distributed file storage systems such as the Interplanetary File System (IPFS). Interplanetary File System (IPFS) uses content addressing. That is, check what is in the file and share it with all nodes to save the file.
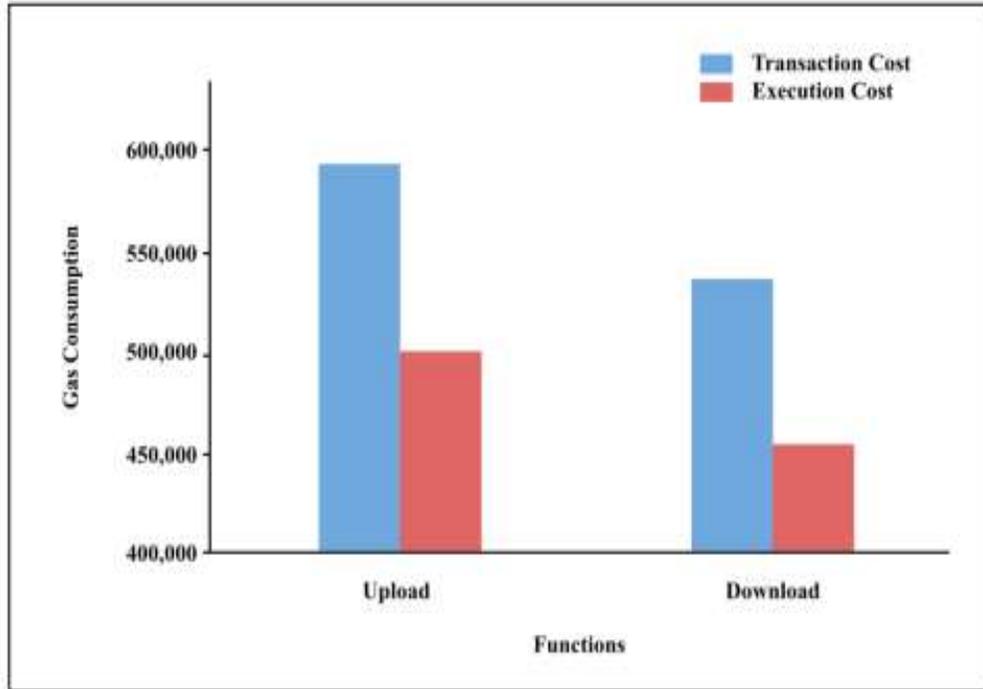
Block chain

A block chain is regarded as a distributed ledger that the records on the chain are maintained by the participating peers. The transaction results are validated by the peers and are linked together by utilizing cryptographic mechanism. The first example of a block chain implementation is Bit coin. Bit coin is a digital crypto currency. The main idea of Bit coin is to offer a decentralized banking system. Users exchange their assets and trust the transaction results which are recorded on the distributed ledger. The results are trusted since they are validated by the participants. After the validation, the transactions are transmitted to the block chain which cannot be tampered with. The participants, known as the miners in the block chain network, are rewarded with crypto currency for their computational work. This is so-call an incentive mechanism to validate transactions and thus make a consensus in the network. Since the miners are all anonymous peers, any single miner cannot be trusted to prevent the transactions results are dominated by the minority. Therefore, a consensus mechanism called proof-of-work is introduced to reach an agreement in the block chain network. Generally, a new block contains a set of new transactions, information required to keep track of the history of transactions and the result of a mathematical puzzle.

METHODOLOGY

Our proposal for a secure file sharing system is based on the utilization of permission-less block chain and IPFS, which is a decentralized method of recording transactions. While permission-less block chain allows any user to participate in the network, it presents a challenge when it comes to validating users since there is no trusted central party. This can result in permission issues in the file sharing mechanism. To address this problem, we have designed a distributed access control and group key management system that utilizes the IPFS proxy. The motivation for our proposed system is rooted in the fact that the nodes in the block chain network have memory limitations, and only transaction records can be stored on the block chain rather than complete files. The Block chain and IPFS-based secure file storage and sharing mechanism allows for decentralized, private, and tamper-resistant data management. The process begins with user authentication, in which each user generates a public-private key pair and stores the public key on the block chain while keeping the private key secure. Files are encrypted, separated into chunks, and uploaded to IPFS, with each piece assigned a unique hash for integrity verification. Block chain-primarily based totally record garage and sharing is an exceptionally new concept, and plenty of humans aren't acquainted with the generation.

RESULTS AND DISCUSSIONS

The proposed hybrid file-sharing model's implementation demonstrated positive efficiency, security, and usability outcomes. The approach effectively addressed the shortcomings of traditional centralized file-sharing platforms by merging decentralized file storage and access control with centralized user management. Users can share files with this system without interacting directly with complex block chain technologies. Using centralized user management improves user accessibility and reduces entrance barriers. Data redundancy and fault tolerance were ensured via IPFS for file storage, reducing the possible data loss compared to a centralized storage server. Files could only be accessed by authorized users, and the permissions were immutably and transparently enforced on the block chain. Using this strategy, data breaches and unauthorized access could be reduced.

Graph 1: Gas Consumption for the Smart Contract

In Graph 1, we have described how much gas is used per function; as shown in the figure, the upload function required more gas as it had to put the data into the blockchain, which took more time to create a block.

Graph 2: Performance Metrics Report with 22k Users in 15 Seconds, Generated by Loader.io

Graph 3: Performance Metrics Report with 2500 Users in 1 Minute, Generated by Loader.io

We have conducted performance tests based on the user using the system simultaneously. In figure 6, we can see that at 00.12 seconds, 2000 users are using the system, and the waiting time is approx. 65ms, which means when they load the system, it will take 65ms to show the results to them. We performed the test many times and found that the average response time is 78ms when 226132 users access the system for 15 seconds and 55ms when 2500 users access the system simultaneously for 1 minute, which is a good benchmark. The results are given in Graph 2 and Graph 3.

CONCLUSION

Our research culminated in the development of "Secure Cloud File Sharing System," a novel block chain-based file sharing system. This innovative platform addresses the critical concerns of data privacy and control in today's digital landscape. This system leverages the power of Ethereum block chain and IPFS to create a decentralized architecture that prioritizes data security. Encryption safeguards user data confidentiality, while the immutability of the block chain ensures the integrity of file-sharing activities. Simulations demonstrated the system's effectiveness in preventing unauthorized access and maintaining data availability. While further optimization might be necessary for handling particularly large files, Secure Cloud File Sharing system presents a promising solution for individuals and organizations seeking a secure and transparent alternative to traditional cloud storage. Its decentralized nature empowers users with greater control over their data, fostering a future of trust and transparency in data sharing. By combining block chain technology with the Inter Planetary File System (IPFS), this study presents a safe and decentralized method of file sharing. Our technology uses block chain-based smart contracts and encryption approaches to improve data security, privacy, and access management. Our technology removes single points of failure and guarantees that sensitive data is protected without relying on a central authority, in contrast to conventional file-sharing techniques that rely on centralized storage. By using block chain-enforced permissions and group-based encryption, the system guarantees safe access control.

References

1. Peng Kang (2022), "Block chain Private File Storage-Sharing Method Based on IPFS", Sensors, ISSN: 1424-8220, vol.22, Issue.(14), https:// doi.org/ 10.3390/ s22145100

2. Devesh Solanki (2021), "EzShare: An Android File Sharing System Using Block Chain & IPFS", International Journal of Creative Research Thoughts, ISSN: 2320-2882,Volume.9,Issue.5

3. Wanzong Peng (2024), "An efficient block chain-based framework for file sharing", Scientific reports, ISSN: 2045-2322,vol.14,doi:10.1038/s41598-024-69011-4

4. Niraj Wadile (2023), "Decentralized File Storage (Interplanetary File System) using Block chain", International Journal of Engineering Research & Technology,ISSN: 2278-0181,Volume.12,Issue.03

5. Prathmesh Doni (2024), "Block chain Based Secure Cloud File Sharing System", International Journal of Research Publication and Reviews, ISSN 2582-7421,Vol.(5),Issue.(5),Pages.9414-9418

6. Dr. Neeta P. Patil (2025), "Secure File Sharing Using Block chain and IPFS with Smart Contract-Based Access Control", Journal of Information Systems Engineering and Management,ISSN:2468-4376,vol.10,issue.16s

7. Anurag Rathour (2024), "Decentralized File System (Storage and Sharing) Using Block chain", International journal of advance research and innovative ideas in education,ISSN:2395-4396,Vol-10,Issue-3

8. Saumyaranjan Sahoo (2022), "Block chain for sustainable supply chain management: trends and ways forward", Electronic Commerce Research,ISSN: 1572-9362,Volume.24,pages.1563–1618

9. Jayendra Kumar (2025), "Blockchain Based Inter-Organizational Secure File Sharing System", International Journal Of Engineering Innovations And Management Strategies,vol.1,Issue.6

10. Smita Athanere (2022), "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing", Journal of King Saud University - Computer and Information Sciences,ISSN:2213-1248, Volume.34,Issue.4