The Journal of Desk Research Review and Analysis, Vol. 1, Issue II, 2023, 121-133
.

BLOCKCHAIN-BASED SECURE DISTRIBUTED FILE STORAGE FOR COMMUNITY CLOUD COMPUTING

TMKK Jinasena[1] and BPS Nayanathara[2]

Abstract

Cloud storage is the most used option for storing and sharing files. However, cloud storage has issues like lack of transparency, privacy, security, and trust. On the other hand, local file storage is always faster and more secure than public cloud storage. Besides, a community cloud is more economical and scalable than private storage. However, due to the ad-hoc nature of community users, developing such a community cloud storage has always been a challenge due to data privacy, security, and availability concerns. Recent developments in blockchain technology and computer security are promising to resolve most of these challenges. Thus, in this research, we are presenting blockchain-based, distributed file storage for community cloud computing. This research, which focuses on local communities, allows them to securely share the excessive storage with the locals to earn something while gaining access to faster, more reliable large-scale local storage. By replacing the central authority of third-party storage vendors and migrating to distributed file storage, local communities will achieve greater security, reliability, and control over their data while reducing the risks of data failures and interruptions. Due to symmetric encryption, data privacy would be 100% assured even though they are stored in other peoples' computers. Moreover, this system uses Reed Solomon. Using the Reed Solomon algorithm, the system can retrieve files even when users holding 33.33% of the files are not present. Besides, it allows local communities to make effective use of their idle and unallocated computer resources transparently.

Keywords: Blockchain, Cloud Storage, Distributed Computing

[1] Senior Lecturer, Department of Computer Science, University of Sri Jayewardenepura
Email: kasun@sjp.ac.lk https://orcid.org/0009-0003-9738-6885

[2] Department of Computer Science, University of Sri Jayewardenepura
Email: sanduminiinayanathara1@gmail.com https://orcid.org/0000-0003-0931-6741

Accepted the revised version: 02 December 2023

Introduction

The world is rapidly developing, introducing new technologies and generating more and more data. Data is the oil of the 21st century. Hence, storing these data securely and accessing them when necessary are major concerns of most of its users. Cloud storage is the most popular method of storage at present. However, it comes with numerous issues such as privacy (Akremi & Rouached, 2021, pp. 7956-7988), security (Thakkar & Shah, 2021, pp. 466-478), transparency, and trust (Suresha & Vijatakarthic, 2020). Authors (Parikh et al., 2019, pp. 734-736) have listed security issues in the three cloud service architectures - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS). Thus, people research more powerful technologies that can handle a large amount of data without such issues. However, we already have a decent amount of idle or unallocated computer resources within our computers. Local communities like universities, companies, schools, and laboratories possess a relatively large sum of idle or unallocated resources. An example of a vast decentralized and distributed network is the Internet. Cloud storage is also considered less expensive and more dependable than local storage as it has a lower risk of data loss. The behaviour of cloud storage, in simple terms, is the process of data being stored in remote storage, which is maintained and secured by a third party instead of the data owner's hardware. This means much of the data on the Internet is in the possession of a few cloud service providers thus making it centralized. As a result, although the cloud storage system is a great discovery that immensely contributed to advancing the data storing mechanism, there are many security and privacy (Akremi & Rouached, 2021, pp. 7956-7988) issues behind it.

The main problem is the inability to guarantee users' privacy due to the involvement of a third party, as shown in (Kadhim et al., 2018) and (Mollah et al., 2017, pp. 38-54). The present cloud storage architecture is not fully distributed. Thus, any breakdown or attacks on servers would result in massive amounts of data losses, resulting in data security issues. The attack on Amazon Web Services in February 2020 is an example. Lack of transparency, trust, and control over stored data are some more issues (Kadhim et al., 2018), (Charanya & Aramudhan, 2016, pp. 1-4).

A decentralized model for data storage utilizing blockchain technology can solve the security issues of cloud storage while utilizing idle and unallocated computing resources. This blockchain-based decentralized model is horizontally scalable; thus, we can add more nodes or machines to the system, thereby increasing the capacity of the system while utilizing existing machines and PCs in our local environment. Users can get registered into the system by renting out their unused disk space to the system. So, this system also paves the way to make some earnings from their idle and unallocated disk spaces in PCs. Files uploaded to be stored in this system are encrypted, sharded, replicated, and distributed to nodes connected.

Blockchain is a peer-to-peer network that acts as a shared, unchangeable record, making recording transactions and tracking assets easier. This system uses Blockchain technology to keep track of transactions. With the use of blockchain technology, the system was able to utilize characteristics of blockchain, like transparency and immutability, to make the system more secure, transparent, trustworthy, and available, which were some of the main issues in the current cloud storage. All the agreements to be carried out between the system and the users are deployed in the blockchain as smart contracts. Those smart contracts are used to keep track of the disk spaces shared by the users, transactions happening between the users, and many more activities. All those transactions are automatically triggered when the defined requirements and conditions are met without any involvement of third parties. Thus, this system is much more secure, transparent, trustworthy, and reliable than the existing file storage systems due to the use of blockchain.

This blockchain-based decentralized file storage system, which is proposed and implemented, is more secure, efficient, and dependable than traditional, centralized cloud storage and much less expensive. Even though this mechanism can extend even for distributed processing, this research was only focused on sharing the storage of devices.

Literature Review

This section discusses the background necessary for the paper and related work.

Blockchain and Smart Contracts

Blockchain is a decentralized ledger of transactions validated over a peer-to-peer network, which was first put into place with Bitcoin (Nakamoto, 2008) by S. Nakamoto. A blockchain gathers data together in groups, also known as blocks. Each block is given an exact timestamp; thus, a block is set in stone when added to the chain, making it immutable. Each record in a blockchain is encrypted individually, making it highly secure.

Due to the blockchain technology's key properties like decentralization, persistency, anonymity, and audibility, as mentioned by the authors (Zheng et al., 2017, pp. 557-564), this technology is used to record and track assets involved in the supply chain (Dutta et al., 2020, p. 102067), financial transactions, voting systems, healthcare applications (Mcghin et al., 2019, pp. 62-75) and IoT-based systems (Sultana et al., 2020, p. 488).

As stated by the authors (Hewa et al., 2021, p. 102857), smart contracts are self-enforcing and self-executing programs that activate the terms and conditions of a particular agreement or contract using software codes and computational infrastructure. The critical importance of smart contracts is the ability to execute peer-to-peer and independently without relying on a centralized third party on agreed conditions, making them more reliable and smarter than paper agreements. The agreement is automatically executed if the protocols are satisfied. The authors of (Buterin et al., 2014) mention the elimination of a trusted third party, forge resistance, transparency, autonomous execution, and accuracy as the key features of blockchain-based smart contracts. A comprehensive overview of blockchain-based smart contracts is provided by the authors (Wang et al., 2018, pp. 108-113) while highlighting the significant issues in smart contracts as well as potential trends.

Ethereum was introduced by Vitalik Buterin (Buterin et al., 2014), who addressed some limitations of Bitcoin's scripting language. Ethereum is a blockchain-based cryptocurrency platform that allows smart contracts to be created and deployed and is based on using tokens, which can be bought, sold, or traded. Real-life assets such as properties, certificates, or currencies are digitally tokenized on the blockchain using smart contracts. The tokenization of assets opened new and more enjoyable, easier, and faster methods of carrying out activities like fundraising, open-sourcing, crowdfunding, and enticing investors. Tokens are built on top of cryptocurrencies using intelligent contracts and, thus, are not native cryptocurrencies. For example, ETHER(ETH) is the native cryptocurrency of Ethereum, and Chainlink(LINK) is a token built on top of ETH. These Ethereum-based tokens are smart contracts that follow the ERC20 Token Standards; thus, these tokens are also known as ERC20 tokens. The authors give a brief overview of blockchain technology, Bitcoin, and Ethereum (Vujicic et al., 2018, pp. 1-6).

Cloud Storage Systems

Users can utilize cloud storage to store and distribute data over the Internet. Here, data is stored in remote storage, maintained, and secured by a third party instead of the data owner's hardware. Unlimited data storage space, convenient, safe, and efficient file accessibility and offsite backup, remote access to

data stored, and low cost of use due to the pay-as-you-go concept and no physical device maintenance being needed are some advantages of cloud storage.

As cloud storage providers store data in high densities in their data centres, any failure in one data centre will lead to substantial data losses. Also, data stored in cloud storage are controlled by a third party. Due to these characteristics of cloud storage, security and privacy issues are inevitable. Authors (Odun-Ayo et al., 2017, pp. 29-34) listed cloud storage deployment, virtualization and availability of cloud storage, data organization, data duplication, data migration, and load balancing as issues related to cloud storage services.

Related Work

The authors (Sirimanna & and Jinasena, 2019) proposed a blockchain-based voting system for decision-making in government policies and projects, further showing how high-security standards of blockchain can be used in crucial government activities of a country. This proposed voting system has utilized and displays well how important blockchain characteristics are and how they can be utilized efficiently. The transparency of blockchain will help achieve credible democracy, and it will bring more positive votes as the reliability of the system is improved. As mentioned in (Sirimanna & Jinasena, 2019), security is the most critical factor in voting, and blockchain can provide it as blockchain has a robust security mechanism. In voting systems, malicious actors can interfere and change the results. This is where blockchain comes to help. Other than that, blockchain transactions are anonymous, thus providing privacy for voters.

Authors (Mithsara & Jinasena, 2020, pp. 72-81) proposed a crowdfunding and decision-making platform for major projects in the public and private sectors using blockchain technology. This proposed platform helps to invest in large business projects despite the lack of trust and issues with the existing investment methods. Agreements and votes are written in the blockchain; thus, they are immutable, and the execution of agreements happens without the involvement of humans; thus, the reliability and security of the system are higher. Both (Sirimanna and Jinasena, 2019) use blockchain characteristics effectively and show how blockchain can solve different real-world issues.

The authors of the paper (Javed et al., 2021, pp. 41129-41143) are a new technology that uses blockchain and smart contracts to improve privacy. Here, data is securely stored in a distributed way and processed in a trusted execution environment chosen by the user. A medical data-sharing project was forwarded (Shen et al., 2019, p. 1207) with the use of blockchain, digest-chain, and structured P2P network techniques.

Research on developing blockchain-based file storage can be found in the past. The authors of (Wilkinson et al., 2014) proposed a blockchain-based P2P cloud storage network named Storj, which enabled data to be shared without needing a third-party supplier and was end-to-end encrypted. Storj allows users to rent out spaces on their hard drives. Users that contribute storage space will be rewarded in their cryptocurrency Storjcoin X (SJCX), with the reward amount varying based on the magnitude of the donation and time provided. Storj stores the metadata on the Ethereum blockchain, allowing users to retrieve their complete data anytime they need it.The authors forwarded a blockchain-based security architecture for cloud storage named Block-secure. This project focused on data security when using blockchain to store files in the cloud.

Sia is another blockchain-based storage platform that was forwarded (Vorick & Champine, 2014, p. 2018) by Vorick and fellows. Sia is similar to Storj, but Sia runs on its blockchain and uses SiaCoin (SC) as its native cryptocurrency. Another decentralized storage network introduced by the study is

FileCoin (Benet, 2017). It runs on top of the InterPlanetary File System (IPFS). Tokens used in FileCoin transactions are Filecoin (FIL). describes how these systems work, and compare those storage systems with cloud storage networks. Here, the above-mentioned storage systems, Storj, Sia, FileCoin, and Swarm, are considered in their survey. However, all these proposed cloud-based storage systems focused their implementations on Wide Area Networks. However, the blockchain-based decentralized file storage system forwarded here is mainly optimized for the Local Area Network. Also, this enables local communities to use their extra computing resources, thus optimizing the use of already available resources.

According to the literature survey, all the proposed cloud storage systems were focused on Wide Area Network implementations. Nevertheless, this paper proposes a cloud storage system using smart contracts to be implemented in a Local Area Network. The spare disk spaces of the users connected to the system will be utilized as the system's storage.

Methodology

Analyze the Need for Solutions to Solve Cloud Storage Issues

Cloud storage is the most popular option for storing files nowadays. However, the issues with the existing cloud storage have been discussed in previous chapters. Lack of privacy, transparency, trust, and security are some key issues in cloud storage. So, a better solution that can store files without facing such issues is introduced through this project. This solution utilizes a collection of well-recognized technologies like blockchain and distributed computing. Other than that, this suggested solution makes use of the already available computing resources that are idle and unallocated. As mentioned, although the cloud storage architecture is distributed, the data is still stored at high density at several data centres. Thus, any breakdown or attack would result in massive data losses and data security issues. Therefore, storing data in a distributed manner can help in securing data. Thus, distributed computing was used. Besides that, blockchain and concepts like encryption, file chunking, and replication are further used to solve cloud storage issues. Blockchain is a well-recognized technology for its characteristics like security, transparency, and trust, which also helped enhance the quality of this solution.

Design

This section will give the high-level architecture and an overview of the proposed distributed file storage based on blockchain. The main activities between the user and the distributed file storage are shown in Figure 1.

This File Storage System performs the following tasks.

1. Store files - When files are stored in the system, those files are encrypted using symmetric encryption, and then those encrypted files are split into six pieces. These pieces of files are then distributed among the nodes in the P2P network. The metadata related to where these file pieces will be stored in a distributed database like Cassandra.
2. Retrieve files - When a user requests to retrieve a file he/she has stored in this storage system, the system will first investigate where the file chunk of the requested file is to be found. Then, these file chunks will be retrieved to reconstruct the original file, which will be decrypted back.
3. Pay for usage and rewards - Whenever a user stores a file in the system, he/she should pay tokens to the system according to the size of the file that is being stored. The system will pay when storing files in some users' shared disk space. Rewards will also be given to users timely.
4. Share disk space - A user can share disk space with the system. Every user joining the system should contribute a predefined minimum amount of disk space to the system.

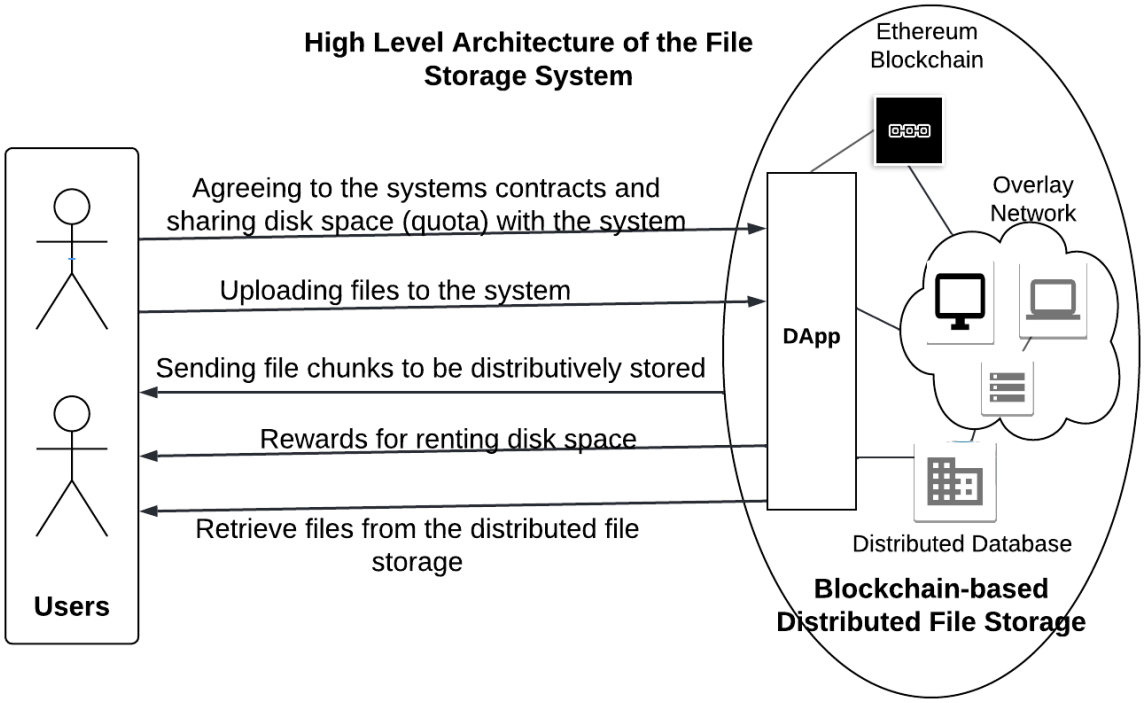

Figure 1: Overview of the Distributed File Storage System

How the file storage system work?

Figure **2** shows the flow of processes when uploading and retrieving a file. A user joins the distributed file storage system by agreeing to share the system-defined minimum required amount of disk space with the system. The users will then be able to upload their files to the storage system to be stored.

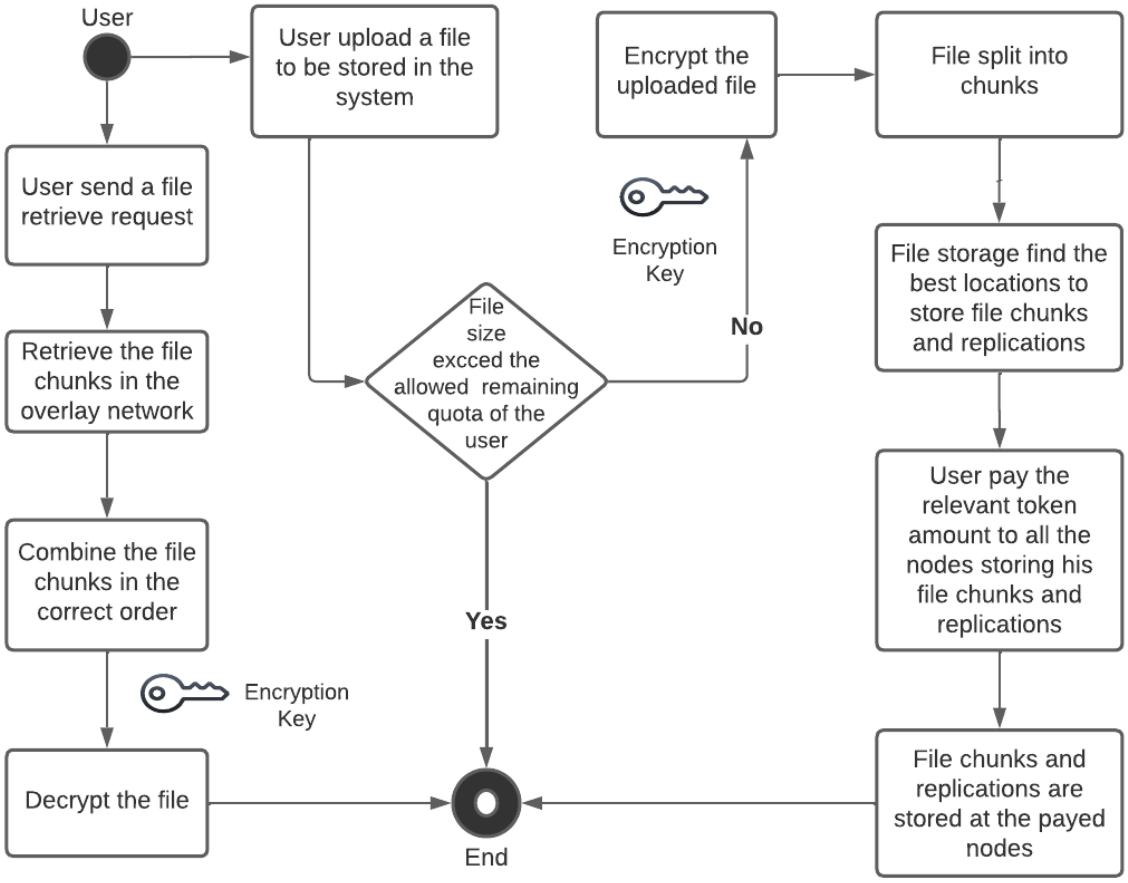

Figure 2: File Upload and Retrieve Process

Files are Encrypted and Chunked

For security, all the files that are uploaded to the File Storage system are encrypted at the source computer itself before they are uploaded. Symmetric encryption is used in the encryption process as the user will only want to decrypt the file. Unique keys are used to encrypt each file, as using the same encryption key for every file can risk all the files if the key to access one file is found.

All the files stored in this system are chunked into six parts. Then, these file chunks are distributed throughout the nodes in the overlay network. Therefore, no node in the overlay network has a complete file with them but a chunk of the original file.

Fault Tolerance and Replication

When a failure occurs, a sound distributed system should continue to work by tolerating the failure without affecting the system's overall functionality. This ability of a system to continue operating even when failures occur is referred to as fault tolerance.

Anytime a node can be unavailable due to being temporarily offline or permanently offline, resulting in system failures or a node in the network crash. To face situations where any given number of nodes are unavailable, this system uses the strategy of replication or redundancy. Here, in replication, copies of each file chunk are made and distributed in the overlay network. Replication improves the durability and fault tolerance of the system.

Use of Reed Solomon Algorithm

Error-correcting codes or erasure coding is a data protection mechanism. Error-correcting codes break data into fragments and encode them with redundant data pieces, which are then stored across a set of drives in different locations. Then, the data is reconstructed using the segments stored across drives at any kind of drive failure or data corruption.

Constraints and Conditions Used in Smart Contracts

1. For the proposed system to accept anyone as a user, the amount of disk space they are willing to rent to the system must be equal to the system's predefined amount of disk space to be rented by a user.

   Disk space shared by the user at signup = a

   Minimum disk space required at signup = b

   $$a >= b \qquad (1)$$

2. Users will receive tokens according to the amount of disk space the user shares with the system. This proposed file storage system uses an ERC20 token of its own named THYME(THM) to keep track of the transactions.

   Value of a token in GB = c

   The amount of tokens a user receives at signup = d

   $bonus$ is an amount predefined by the system

   $$d = [a + (a * \boldsymbol{bonus})]/c \qquad (2)$$

3. Users are allowed to store files only until the total size of the files uploaded amounts to the corresponding value of the user's initial token.

   The cumulative size of all the files stored by the user in the system = e

   $$e <= d * c \qquad (3)$$

   Therefore, according to Equation 2 and Equation 3, a particular user is allowed to store even exceeding the amount of disk space that the user has shared with the storage system.

4. Whenever a user stores a file in the file storage system, that user will have to pay a cost valuing the size of the file that is being stored in the system using the ERC20 tokens the user already has.

   $$Service\ Fee = Size\ of\ File\ Uploaded/c \qquad (4)$$

   This service fee will be distributed among the nodes responsible for storing the user's file chunks as a receipt for those nodes.

   Size of the file chunk received by a node from the system to be stored = f

Receipt = g

Service Fee = h

$$Receipt = f/c \qquad (5)$$

$$Total\ amount\ of\ tokens\ with\ a\ user = d + g - h \qquad (6)$$

5. Users will receive rewards for sharing their disk spaces with this system. However, the smart contract will decide the rewards a user receives depending on the user's availability and the amount of disk space the user has agreed to share with the system. Availability of a user means how often the user is actively connected to the system. If a user is disconnected from the system most of the time, although the user agrees to share disk space with the system, that space is useless as the user is not available to make any use of that disk space. Therefore, the availability of a user is measured by the number of failed attempts that have been recorded when retrieving back files from the user.

   Number of successful retrievals = i

   Number of total retrieval attempts = j

$$Availability = i/j \qquad (7)$$

The user will receive rewards if conditions defined by the system are met at the time of rewards distribution.

Minimum availability percentage to receive rewards = k

$$Availability * 100\% > k \qquad (8)$$

If a user satisfies the condition in Equation 8, that user is eligible for rewards. The amount of rewards a user receives is given by Equation 9.

The total amount of tokens with a user = m

$reward\ rate$ is an amount predefined by the system

$$Reward = m * Availability * \mathbf{rewardRate} \qquad (9)$$

An example implementation of a file upload function that can be written in smart contracts is shown in Figure 3

```
function uploadFiles(address recipient, uint fileSize) external { //diskSpace in GB

  Token thyme = Token(addressThyme);


    uint rental = fileSize;

    require(fileSize > 0, "fileSize cannot be 0");
    require(thyme.balanceOf(msg.sender) >= rental, 'rental exceeds the token balance');
    require(providedDiskSpace[recipient] >= fileSize , 'no enough disk space in the receiver');


    thyme.transfer(recipient, rental);
    providedDiskSpace[recipient] = providedDiskSpace[recipient] - fileSize;


}
```

Figure 3: An example implementation of the file upload function

Results

For each transaction made through the blockchain, a gas fee is charged. The gas fee is the Ether (ETH) required for an Ethereum blockchain network user to conduct a transaction on the network. Figure 4 shows the gas fee charged by a user at an upload transaction function.

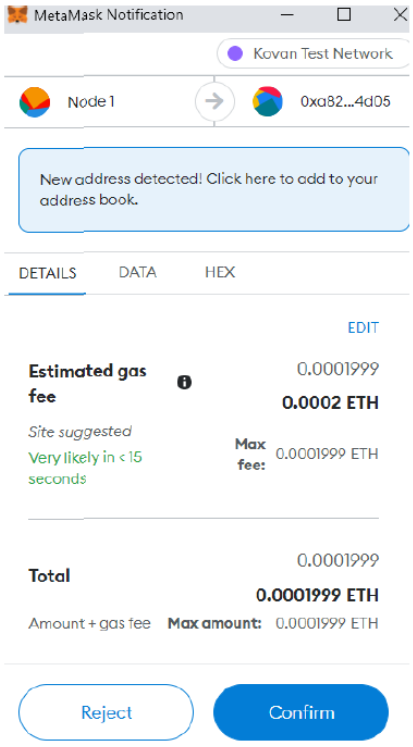

Figure 4: Instance of an upload transaction with the Gas Fee and approximated time taken

Figure 5 shows the average time taken and estimated gas fees charged for the file storage functions. As all the transactions are verified through smart contracts, the time taken for those transactions is slightly higher than the current cloud storage.

Function	Average time taken for the completion	Average gas estimation for the completion
Sign Up	12 s	0.00051 ETH
Share disk space with the system	12 s	0.00051 ETH
Upload file	18s	0.00021 ETH
Retrieve file	13s	0.00019 ETH

Figure 5: Average time and estimated gas taken by the storage system

Using Reed Solomon codes, each file is chunked into six equal pieces. Furthermore, the Reed Solomon algorithm can restore a file to get back the original file even if two chunks of those six chunks are completely lost or corrupted.

Analysis

Authentication Vulnerability, Transparency, Fair Treatment

Each user is identified and authenticated by the system using blockchain. The system will register a user only if the user fulfils the required conditions. That is only if the user agrees to share the minimum amount of disk space requested by the system. Whenever a user logs into the system, the smart contracts will check whether that particular user is registered.

All the agreements and conditions that are to be executed between the users and the system are written in smart contracts. As blockchain is a write-once technology, once data is written into it, that data becomes immutable. Thus, there is barely any chance of someone faking their identity to log into the system or barely any chance of a registered user disguising himself as an unregistered user to the system. Other than that, smart contracts are automatically executed without any intervention from third parties. Thus, all transactions are transparent and trustworthy, and it can be guaranteed that every user is treated the same way. As blockchains are immutable, smart contracts cannot be changed maliciously.

Likewise, users can upload files only up to the size granted by the storage system. The amount of upload size granted to each user is calculated by a smart contract. The number of rentals when uploading files and rewards given to a particular user are all calculated and executed by smart contracts. Therefore, besides authentication due to the use of smart contracts, other functions of the system are also performed securely and transparently.

Uploaded File Security

All the files are encrypted and chunked before being uploaded to the system. Thus, no peer in the file storage system has direct access to a complete file and even the file chunks the user can access are encrypted. Also, any non-owners of a particular file-making file retrieval request will be declined from the system as it will check the meta mask address that the retrieve request was made from in addition to the credentials of the requester.

Another strategy used to ensure uploaded file security is replications. This strategy helps to recover file chunks. Replications of file chunks will be stored in the system as backup file chunks to be used during peer unavailability.

With the use of Reed Solomon code, the storage system can restore files if the files are corrupted or if some data is lost during the transmission of the file. This File Storage system, with the use of Reed Solomon code, can recover the original file even if 33.33% of the file is completely lost or corrupted.

Idle and Unallocated Computer Resource Utilization

Data collected from 50 people through a questionnaire revealed that 73% of people have spare disk space in their laptops and PCs. Therefore, such spare computer resources can be utilized with a system like this.

Conclusion

This idea of developing a blockchain-based secure and distributed file storage system is a much cheaper, faster, transparent, trustworthy, and easier option to use in local communities than using cloud storage services or buying new devices for storage activities.

The immutability and automatic execution of smart contracts make this file storage system more transparent and reliable than cloud storage, as no third parties are involved. Those above-mentioned characteristics and the distributed nature of smart contracts make this file storage system accessible to problems like being subjected to central point failures and lack of control over stored data, privacy, and transparency, which the current cloud storage suffers from. The use of encryption ensures privacy, as no one else can read someone else files. Also, using file chunking replications along with Reed Solomon has increased the security of the files stored. Those concepts make it possible to recover and restore a file at times of issues to the system, like file corruption and node breakdowns.

Most importantly, this file storage system is an ideal way of optimizing idle and unallocated computer resources already available to us. This saves money and resources and paves a way to earn money from spare computing resources.

Future work

This project only focuses on implementing distributed storage, but this solution can also be extended even for distributed processing. With distributed processing, PCs connected to the distributed system can perform processing activities like calculations and model training. This distributed file storage system is optimized for use in a local community like a university or a company. Nevertheless, this can be developed to be networked among several local communities. As an example, file storage systems in several universities can be networked together. Many more functions and features can be added to this system to improve its usability and user experience.

References

Akremi, A., & Rouached, M. (2021). A comprehensive and holistic knowledge model for cloud privacy protection. *The Journal of Supercomputing*, *77*(8), 7956–7988. https://doi.org/10.1007/s11227-020-03594-3

Benet, J. (2017). Filecoin research roadmap for 2017.

Buterin et al. (2014). Ethereum: A next-generation smart contract and decentralized application platform.

Charanya, R., & Aramudhan, M. (2016). Survey on access control issues in cloud computing. *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS).* https://doi.org/10.1109/icetets.2016.7603014

Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research. Part E, Logistics and Transportation Review*, *142*(1), 102067.

Hewa, T., Ylianttila, M., & Liyanage, M. (2020). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857.

https://doi.org/10.1016/j.jnca.2020.102857

Javed, I. T., Alharbi, F., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). PETchain: A Blockchain based Privacy Enhancing Technology. *IEEE Access*, 1–1. https://doi.org/10.1109/access.2021.3064896

Kadhim, Q. K., Yusof, R., Mahdi, H. S., Ali Al-shami, S. S., & Selamat, S. R. (2018). A Review Study on Cloud Computing Issues. *Journal of Physics: Conference Series*, *1018*, 012006. https://doi.org/10.1088/1742-6596/1018/1/012006

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

Mithsara, M., & Jinasena, T. K. (2020). Blockchain-based distributed secure crowdfunding and decision-making platform for large-scale business projects in public and private sectors. European Modern Studies Journal, 72-81.

Mollah, M. B., Azad, Md. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, 38–54. https://doi.org/10.1016/j.jnca.2017.02.001

Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. In *bitcoin.org*. https://bitcoin.org/bitcoin.pdf

Odun-Ayo, I., Ajayi, O., Akanle, B., & Ahuja, R. (2017, December 1). *An Overview of Data Storage in Cloud Computing*. IEEE Xplore. https://doi.org/10.1109/ICNGCIS.2017.9

Parikh, S., Dave, D., Patel, R., & Doshi, N. (2019). Security and Privacy Issues in Cloud, Fog and Edge Computing. *Procedia Computer Science*, *160*, 734–739. https://doi.org/10.1016/j.procs.2019.11.018

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. *Applied Sciences*, *9*(6), 1207. https://doi.org/10.3390/app9061207

Sirimanna, I. S., & Jinasena, T. K. (2019). Blockchain-based, secure, reliable, and distributed voting system for decision making in government policies and projects. ICITR International Conference.

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., & Javaid, N. (2020). Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Applied Sciences*, *10*(2), 488. https://doi.org/10.3390/app10020488

Suresha, K., & Vijatakarthic, P. (2020). A comprehensive review on trust issues, security, and Privacy issues in cloud storage. International Journal of Innovative Science and Research Technology.

Thakkar, V., & Shah, V. (2021). Investigation of techniques used for mitigating security and privacy issues in cloud-based electronic health record(EHR) systems. *International Journal of Innovative Science, Engineering & Technology*, *8*(2), 466-478.

Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March 1). *Blockchain technology, bitcoin, and Ethereum: A brief overview*. IEEE Xplore. https://doi.org/10.1109/INFOTEH.2018.8345547

Vujicic et al. (2018). Blockchain technology, bitcoin, and ethereum: A brief overview. 17th International Symposium infoteh-jahorina, (pp. 1-6).

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An Overview of Smart Contract: Architecture, Applications, and Future Trends. *2018 IEEE Intelligent Vehicles Symposium (IV).* https://doi.org/10.1109/ivs.2018.8500488

Wilkinson et al. (2014). Storj is a peer-to-peer cloud storage network.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress).*