

Decentralized Storage System to Store Data using Blockchain Technology

Akshar Mehta
Computer Engineer

MCT's Rajiv Gandhi Institute of Technology
Mumbai, India
mehtaakshar1234@gmail.com

*Sunil Khachane
HoD, Computer Department
MCT's RGIT
Mumbai, India
sunil.khachane@mctrigit.ac.in

Sakshi Pandey
Computer Engineer
MCT's Rajiv Gandhi Institute of Technology
Mumbai, India
sakshi27p@gmail.com

Karan Parmar
Computer Engineer
MCT's Rajiv Gandhi Institute of Technology
Mumbai, India
parmarkaran1976@gmail.com

Nilesh Sahu
Computer Engineer
MCT's Rajiv Gandhi Institute of Technology
Mumbai, India
nileshsahu790@gmail.com

Abstract—In today's society, data storage is becoming more and more crucial. In the lives of customers, data reliability, secrecy, security, and accessibility have all been crucial factors. All web2.0 vulnerabilities are removed by blockchain in general by introducing new technology and structure. With the power of the blockchain, data storage problems might be resolved and customer privacy and security of their data could be guaranteed. This reduces the possibility of a single point of failure and encourages ideas like tokenization and incentivization to reward customers and storage providers for making data storage compatibility possible. As a result, we offer a decentralised storage system that use a blockchain network and smart contracts to store user data.

Index Terms—Blockchain, vulnerability, data storage.

I. INTRODUCTION

Storage is a mechanism that allows a computer to keep data indefinitely or temporarily. Storage devices, such as flash drives and hard discs, are essential components of most digital devices because they allow users to save various types of data, such as images, files, videos, and unprocessed data.

Cloud storage systems have become increasingly popular in recent years to meet the data storage and sharing needs of businesses, organisations, and individuals. Users who invest in these services must fully trust the companies to keep their important and private data secure for an extended period of time. However, centralised systems are more vulnerable to being attacked or having their services severely disrupted. Furthermore, data leakage cases such as Facebook-Cambridge Analytica have resulted in a strong shift away from centralised to decentralised data storage systems at the time.

Cloud computing is the delivery of various services via the Internet. Data storage, servers, databases, networking, and software are examples of these resources. Cloud-based storage enables files to be stored to a remote database as opposed to a proprietary hard drive or local storage device. As long as an electronic device has internet access, it has access to data and the software programs needed to run it.

Because the information being accessed is situated virtually, or in the cloud, cloud computing derives its name. Users can access data via the Internet by storing files and apps on remote servers thanks to cloud service providers. This enables remote working since the user does not need to be in a certain place to access it.

The Internet becomes the cloud, and your data, work, and applications become accessible from any device that can connect to the Internet, wherever in the globe. The cloud can be both public and private. For a fee, public cloud services offer their services over the Internet. Private cloud services, on the other hand, only serve a limited number of people. A network infrastructure called these services offers hosted services. There is also a hybrid option that includes aspects of both public and commercial services.

With cloud computing, all of the labor-intensive data processing is offloaded from the device you carry or sit on while working. Additionally, it offloads all of that work to enormous computer clusters in the internet. Cloud computing is becoming increasingly popular among individuals and businesses for a variety of reasons, including cost savings, increased productivity, speed and efficiency, performance, and security. Google Cloud, Microsoft Azure, Amazon Web Services, and many other platforms already exist as data storage solutions.

The fact that all of this data is kept on one central server increases the possibility of a single point of failure or an assault meant to bring the server down. Large tech businesses make up the existing structure, and a single organisation purchases and offers all services.

When data is kept by a third party, there are significant concerns about data security and confidentiality. Due to a single point of failure, other storage systems are prey to cyber attacks. Large IT corporations might also stop supplying services to the client because they have control and authority over the client's data.

Blockchain storage is a method of storing data in a decen-

tralised network that uses unused hard disk space from users all over the world to store files. Decentralized cloud storage is an alternative to centralised cloud storage and can solve many of the problems associated with centralised systems.

II. LITERATURE REVIEW

Decentralized storage systems have grown in popularity in recent years as a result of its capacity to offer a more secure, effective, and dependable method of data storage and exchange. One of the most well-known decentralised storage systems that has gained widespread acceptance in both the research community and industry is the InterPlanetary File System (IPFS). We will talk about IPFS's primary features, as well as its possible advantages and difficulties in creating a decentralised storage system, in this literature review.

The decentralised storing and sharing of files is made possible by the IPFS protocol. In contrast to conventional centralised storage systems, IPFS distributes and stores data through a peer-to-peer network. Since IPFS is built on content addressing, each file is given a distinct hash, which is then used to locate the file on the network. Since data is duplicated over numerous nodes and may be retrieved even if some nodes are unavailable, this method makes IPFS more resilient to failures.

One of IPFS's key benefits is its capacity to offer a more private and secure method of data sharing and storing. Data is spread among several nodes, making it more challenging for attackers to access it unlawfully. Moreover, IPFS provides end-to-end encryption, enabling data to be encrypted prior to being stored on the network and ensuring that only authorised users may access it.

Another benefit of IPFS is its ability to make data sharing and storing less expensive and complicated. IPFS does not require a centralised server to store and distribute files because it utilises a peer-to-peer network. As a result, it is less expensive to operate a central server and simpler to grow the storage system as necessary. Moreover, IPFS offers incremental updates, which eliminates the need to store and disseminate the full file by only storing and distributing the changes to a file.

Despite the potential advantages of IPFS, there are numerous issues that must be resolved if a dependable and effective decentralised storage system is to be created. The network's scalability is one of the major issues. It gets harder to maintain consistency and make sure that every node has access to the same data as the network grows in size. Moreover, network latency and bandwidth restrictions may have an impact on IPFS performance.

Another concern is the issue of data-availability. It is possible for some nodes to go offline or become inaccessible since data is spread over numerous nodes, making it challenging to retrieve data. Since at least one node in the network holds a copy of the data, IPFS offers content-addressed storage to solve this problem.

An effective technology for creating a decentralised storage system is IPFS, in conclusion. It offers a more dependable, efficient, and secure means to store and share data and may be

less expensive and complex than conventional storage systems. To create a dependable and scalable decentralised storage system using IPFS, there are various additional issues that must be resolved.

III. RELATED WORK

A. Blockchain Technology

Decentralized cryptocurrencies (like Bitcoin, Ethereum, Litecoin, etc.) have gained popularity in recent years, and the blockchain technology that powers cryptocurrencies is receiving increasing attention. The blockchain has recently become very important in the world of finance. It has also been discovered to be helpful in numerous other non-financial domains. Examples include decentralised storage, identity-based PKI, decentralised document existence proof, decentralised IOT, and decentralised supply chains.

A personal data management system based on blockchain technology has been proposed in order to enable data owners to own and control their own data. This system can improve the privacy of user data. A blockchain architectural system for IOT was developed to address the issue of data privacy in IOT systems, and advanced encryption standard (AES) technology was employed to safeguard sensitive data. A blockchain-based access control architecture for increasing the security of big data platforms was presented to address the security and privacy challenges that are impeding the growth of big data.

The use of conventional database techniques to store financial transactions has a number of drawbacks. Take the sale of a piece of real estate as an example. The buyer acquires ownership of the property following the exchange of funds. Both the buyer and the seller are capable of maintaining their own records of financial transactions, but neither can be trusted. It is possible for both the buyer and the seller to claim that money has been made even though it hasn't, and both parties can simply contest this.

Transactions must be monitored and confirmed by a reliable third party to prevent potential legal problems. In addition to making the transaction more challenging, the presence of this centralised authority creates a weak point. Both parties may suffer if the main database is compromised.

Blockchain resolves these problems by developing a decentralised, unchangeable mechanism for transaction recording. Blockchain develops separate ledgers for the buyer and seller in real estate transactions. All transactions are subject to approval by both parties and are automatically updated in both of their ledgers in real time. Any change to previous transactions will reflect poorly on the entire ledger. Due to these features, blockchain technology has proven valuable in a variety of fields, including the creation of digital currencies like Bitcoin.

B. Advanced Encryption Standard Technology

The United States government selected the symmetric block cypher known as the Advanced Encryption Standard (AES) to safeguard sensitive data. To encrypt sensitive data, AES is used in hardware and software across the globe. Cybersecurity and

government computer security are both dependent on it for the protection of electronic data. The Data Encryption Standard (DES), which was becoming increasingly susceptible to brute-force attacks, prompted the National Institute of Standards and Technology (NIST) to identify the need for an alternative in 1997.

The more modern and sophisticated encryption method, according to NIST, must be declassified and able to "secure sensitive government information well into the [21st] century." It was designed to have simple hardware and software implementation, work well in constrained contexts like a smart card, and provide strong protections against a variety of attack vectors.

AES is an iterative cypher as opposed to a Feistel one. Its foundation is a "substitution-permutation network." It consists of a number of interconnected operations, some of which substitute certain outputs for inputs (substitutions), while others require shifting bits about (permutations).

It's interesting to note that AES uses bytes rather than bits for all of its calculations. As a result, AES considers a plaintext block's 128 bits to be 16 bytes. For processing as a matrix, these 16 bytes are organised into four columns and four rows.

In contrast to DES, the number of rounds in AES varies and is based on the size of the key. For 128-bit keys, AES employs 10 rounds; for 192-bit keys, 12 rounds; and for 256-bit keys, 14 rounds. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

IV. PRELIMINARIES

The background information and specific aspects that will be utilized in this article are reviewed in this section.

A. IPFS

Computers all around the world can store and serve files as a part of a sizable peer-to-peer network thanks to a distributed file storage protocol known as the Interplanetary File System (IPFS). Downloading the IPFS software allows any machine to start hosting and serving data from any location in the world. A file uploaded to the IPFS network can be viewed and downloaded by anybody who has IPFS installed on their machine.

With IPFS, there will be just one network in existence. If two users publish a block of data with the same hash, the peers downloading the content from "user 1" and the peers downloading it from "user 2" will exchange data. IPFS aims to displace the technologies now in use for providing static online material by utilising HTTP-accessible gateways.

The way we currently utilise the Web and IPFS are quite similar. A unique cryptographic hash string is created when a file is posted to the IPFS system and can be used to retrieve the content. Similar to a Web Uniform Resource Locator is the hash string (URL). Moving future, the file location will simply be referred to as the hash string. Blockchains are not practical for storing large data due to block bloat and transaction fees (video, audio, etc.).

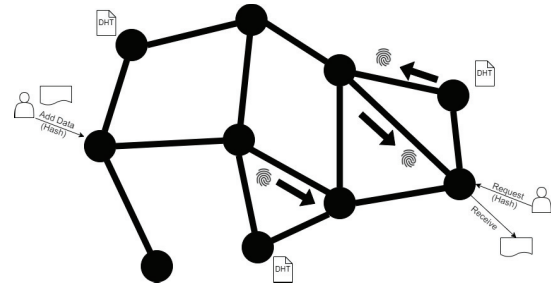


Fig. 1. A simplified IPFS network and its components.

As a result, we store the encrypted file in IPFS according to the plan. In the Ethereum blockchain, a small amount of metadata is stored. Before their attribute set satisfies the access policy defined by the data owner, users won't be permitted to receive data from the Ethereum blockchain, decrypt the file location, download the encrypted file from the IPFS via the file location, and then decrypt it.

B. Transaction life cycle

A transaction needs to be authorised and validated before it can be posted to the blockchain. A transaction must go through several crucial phases before it can be put to the blockchain. We'll focus on cryptographic key authentication, proof of work authorization, mining's role in blockchain networks, and the more recent use of proof of stake protocols.

This lifetime tracks a single transaction as it passes through each step of the blockchain integration process. Simply said, a transaction is the act of transmitting money by one party to another and having that other party accept it. Although conducted digitally, the blockchain transaction is also very comparable. The life cycle of a blockchain transaction includes the following stages:

If there are two Bitcoin users, A and B. A wishes to send B 1 bitcoin.

- A obtains B's wallet address first (a wallet in the blockchain is a digital wallet that allows users to manage their transactions). With this knowledge, he creates a new transaction from his wallet for 1 bitcoins with a 0.003 bitcoin transaction fee.
- He then confirms the data before sending the transaction. Every transaction that is launched has a digital signature from the sender, which is essentially the sender's private key. This is done to increase the transaction's security and guard against fraud.
- The transaction signing mechanism is then launched by A's wallet, signing his transaction with his private key.
- The transaction has now been published to the network's memory pool.
- The miners eventually agree to this transaction. This transaction is grouped into a block by the miners, who also determine the Proof of Work and give the block a hash value before mapping it to the blockchain.
- The Blockchain now has this block.

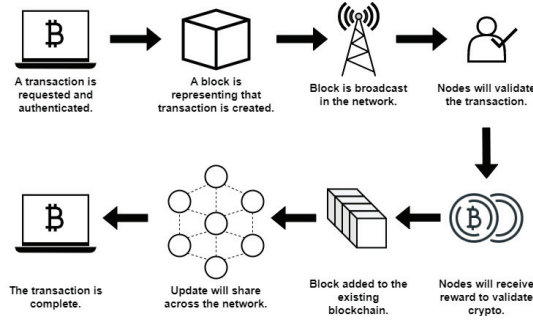


Fig. 2. Blockchain transaction process.

- This block is recognised by the network as a legitimate transaction as it receives confirmation.
- The moment this transaction is approved, B receives his bitcoin.

C. Merkle Tree

The Merkle tree serves as the essential foundation for blockchain technology. It is a form of mathematical data structure made up of hashes of different data blocks that is used to summarise all the transactions in a block of data. It also makes it possible to quickly and securely verify content across a vast body of data. It also helps to verify the data's correctness and comprehensiveness. Both Ethereum and Bitcoin use the Merkle Tree structure. Merkle Tree is also known as "Hash Tree."

A Merkle tree records all of the transactions in a block by generating a digital fingerprint of the full collection of transactions. It allows the user to verify if a transaction can be included in a block or not.

Merkle trees are created by continuously hashing node pairs until there is just one hash left. This hash is the Merkle Root, sometimes referred to as the Root Hash. The Merkle Trees are constructed from the bottom up.

Each leaf node is a hash of transactional data, while the non-leaf node is a hash of its prior hashes. An even number of leaf nodes are required since Merkle trees are in a binary tree. If the number of transactions is odd, the final hash will be copied once to create an even number of leaf nodes. The Merkle Root information can be found in block headers. The block header is the area of a bitcoin block that is hashed during mining. It contains the Root Hash of the most recent block's transactions in a Merkle Tree as well as the Root Hash of the block before that, which is a Nonce. Consequently, by including the Merkle root in the block header, the transaction is rendered impregnable. Each leaf node is a hash of transactional data, while the non-leaf node is a hash of its prior hashes.

An even number of leaf nodes are required since Merkle trees are in a binary tree. If the number of transactions is odd, the final hash will be copied once to create an even number of leaf nodes. The Merkle Root information can be found in block headers. The block header is the area of a bitcoin block that is hashed during mining. It contains the

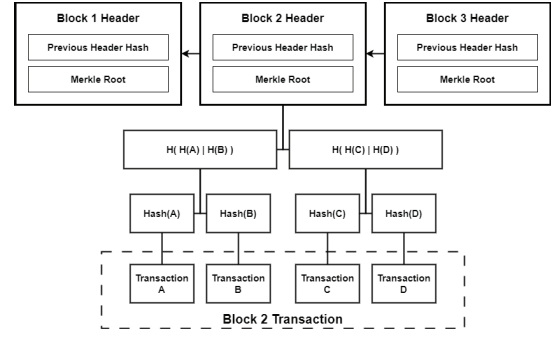


Fig. 3. Blockchain transaction process.

Root Hash of the most recent block's transactions in a Merkle Tree as well as the Root Hash of the block before that, which is a Nonce. Consequently, by including the Merkle root in the block header, the transaction is rendered impregnable.

V. METHODOLOGY

The suggested system runs through six phases:

A. Upload file

The user uploads a file using the file picker. The system verifies the file size and availability of network storage. The file is uploaded once there is enough storage space. The system then moves on to the following phase. Users are informed to try again when adequate storage is not available.

B. File Encryption

AES 256 bit encryption is applied to the submitted file. The user's wallet address is combined with a random salt value to create the encryption key. Data pertaining to users is encrypted using this encryption key and an IV. This guarantees that the user's information is kept secret.

C. File Storage across Multiple Peers

The IPFS protocol is then used to distribute the encrypted file throughout the network in 256KB blocks. To enable registered peers to store the file on the network, the suggested method makes use of a private IPFS network. The file block is duplicated across several peer storages using the IPFS cluster to increase availability. IPFS provides a hash value that shows the path of the file.

D. Reimbursing Peers for File Storage

The total amount of cryptocurrency is calculated and removed from the user's wallet after the file has been disseminated across peers. The user's wallet sends this cryptocurrency first to the smart contract. This sum is distributed by the smart contract to the peers who have saved the user's file.

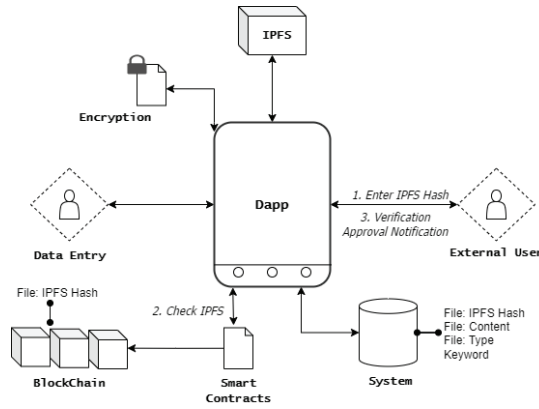


Fig. 4. Verification of the File Upload

E. Storing IPFS Hash value

The user's wallet address, metadata, and the hash value are all stored in the blockchain using a smart contract. Similar to agreements, smart contracts function without the involvement of a third party. They have some degree of control over assets transferred between parties or transactions between nodes. Code snippets are kept on a blockchain network and run automatically when certain criteria are satisfied. For the smart contract to function under our proposed system, there must be sufficient network storage space for files and the user must have enough funds in their wallet to pay their peers.

F. File Upload Notification

The user is then told if the file upload was approved or denied by the blockchain system.

G. Smart Contract - Solidity

The smart contract plays a crucial role in managing the content storage and access. The contract utilizes a mapping mechanism to associate each user's Ethereum address with their respective content ID. This ensures that the content is securely linked to the correct user.

The "storeContent" function is responsible for storing content on the blockchain. It verifies that the content ID is not empty before associating it with the sender's Ethereum address in the mapping. This process ensures the authenticity of the stored content.

On the other hand, the "getContent" function enables users to retrieve their stored content. By calling this function, users can access their content based on their authenticated Ethereum address. The content is retrieved from the mapping and returned to the user, providing seamless content access.

H. Frontend - React + Redux

To create an intuitive and user-friendly experience, our project's frontend application is developed using the ReactJS and efficiently managed with Redux for seamless state management. The application boasts a robust authentication

system, where users are provided with a secure access mechanism through JWT (JSON Web Token) tokens, ensuring safe communication with the blockchain.

Upon successful user login, our application dynamically generates a unique JWT token that serves as an exclusive identifier of the user's authenticated status. This token is then included in every subsequent request made to the blockchain, guaranteeing that only authorized users gain access to their respective content.

To streamline the user experience, our project harnesses the power of the Redux store, managing the authentication state. When a user eagerly clicks the "Get Content" button, a carefully orchestrated action named "getContent" is promptly dispatched from the Redux store. This well-designed action sets in motion an authenticated API call to the smart contract, carrying the JWT token for user verification.

In the heart of our project lies the smart contract, which astutely utilizes the provided JWT token to discern the user's identity and subsequently extract the associated content ID from the mapping. With precision, the content ID is then gracefully returned to the frontend, seamlessly presented to the user. Through this harmonious integration of blockchain and frontend authentication, we assure our users of the utmost convenience in accessing their valuable stored content, ensuring a smooth and secure journey within our platform.

I. Explanation

This cutting-edge algorithm introduces a compelling and user-friendly solution tailored for decentralized content storage and retrieval. By ingeniously combining the formidable capabilities of blockchain technology and frontend authentication, our system delivers an unparalleled level of security and tamper-proof protection for all stored content.

The heart of our system lies in the smart contract, assuring that each user's precious content is meticulously associated with their unique Ethereum address. This meticulous linkage guarantees the utmost data integrity and fortifies the security of our platform, ensuring users can confidently entrust their valuable data to our decentralized storage solution.

To establish an unbreakable trust between the frontend application and the blockchain, we harness the power of JWT tokens. These tokens serve as a secure bridge, facilitating seamless and authenticated communication between the frontend and blockchain. As a result, only authorized users can effortlessly access their respective content, shielding our platform from any unauthorized access attempts.

In essence, our algorithm showcases an unparalleled framework for decentralized content management, empowering users to safely and efficiently store and retrieve their invaluable data. With this innovative solution, users can navigate our platform with the utmost ease and confidence, confident that their data is securely and conveniently stored in our decentralized ecosystem.

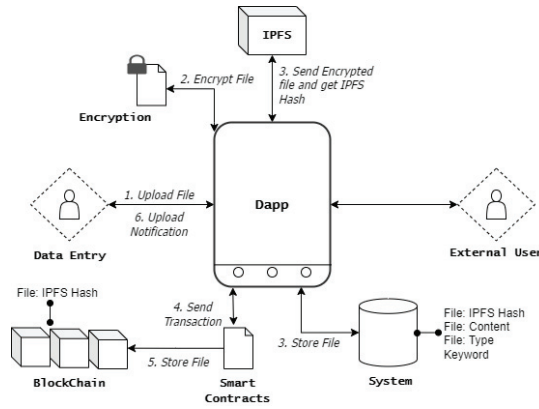


Fig. 5. System Architecture

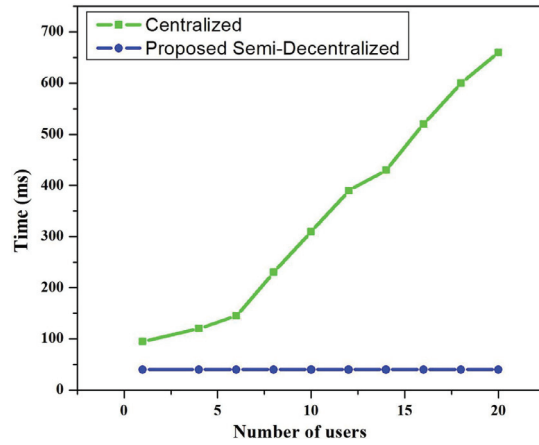


Fig. 6. Result

VI. RESULT

A. Advantages of IPFS for Decentralized Data Storage

Data storage using decentralized IPFS (InterPlanetary File System) technologies is safe and effective. Unlike traditional storage methods based on location, IPFS utilizes content-addressed storage, where data is stored on multiple network nodes rather than a central server.

This approach offers several advantages:

- **Decentralization:** IPFS being a decentralized network, data is distributed across multiple nodes, reducing the risk of a single point of failure and enhancing security.
- **Data integrity:** IPFS stores data based on its content, ensuring data tamper-proofness. Any alteration to the data will generate a new hash, preserving data integrity.
- **Faster data access:** Caching data on network nodes allows for quicker data retrieval, improving overall data access speed.
- **Cost-Effectiveness:** IPFS eliminates the need for expensive servers or data centers, reducing data storage and retrieval costs. Data can be stored on nodes managed by individuals or businesses with extra computer power.

- **Enhanced Data privacy:** Encrypted data spread across multiple network nodes enhances data privacy, making unauthorized access challenging.

B. User-side Decryption Efficiency

The computational burden of user-side decryption was evaluated, and the proposed method demonstrated improved decryption efficiency from the user's perspective. By leveraging blockchain for most computational processes, the suggested approach significantly reduces decryption time. The decryption process only requires simple addition and multiplication operations once the user possesses the decryption keys, making it nearly constant in duration. The number of users in the domain does not impact the decryption time.

Overall, IPFS-based decentralised storage systems offer a safe, effective, and economical solution to store data. It has the potential to completely change how data is accessible and kept, particularly in sectors that demand the highest standards of data security and privacy. Like any new technology, it does, however, have significant difficulties that must be overcome, including scalability, interoperability, and user adoption.

Fig. 6 demonstrates the computational burden of user-side decryption. From the user's perspective, the suggested method delivers better decryption efficiency because blockchain handles the majority of the computational processes. Using the user-associated decryption engine, the domain authority retrieves the ciphertext supplied by the data owner from the block chain during the decryption phase. The final decryption just requires the user to execute simple addition and multiplication operations once they have the decryption keys, so the number of users in the domain has no impact on how long it takes to complete. Decryption time for the user is therefore almost constant.

VII. FUTURE SCOPE

The project opens up exciting possibilities for further enhancements and expansions in the domain of decentralized storage systems using blockchain technology. Some potential future scope and directions for development are as follows:

- **Integration of Different Blockchains:** Exploring the integration of additional blockchains like Solana, Avalanche, or others can enhance the interoperability and versatility of the decentralized storage system. By leveraging the unique features and capabilities of different blockchains, the system can cater to a broader range of use cases and user preferences.
- **Self-Hosted IPFS Nodes:** Setting up and maintaining our IPFS nodes can offer greater control and independence from third-party node providers like Pinata. This self-hosted approach can enhance data privacy, reliability, and reduce operational costs.
- **Integration with Filecoin:** Integrating Filecoin, developed by IPFS, can bring additional benefits to the project. Filecoin's decentralized storage network can complement the existing infrastructure and provide more options for data storage and retrieval.

- Improved User Interface and App Compatibility: Enhancing the user interface and making the project app-compatible can attract a wider audience and improve user experience. Creating user-friendly applications that interact seamlessly with the decentralized storage system can encourage greater adoption and usage.
- Custom Incentive Mechanisms: Designing and implementing custom incentive mechanisms for users who also function as storage providers can foster a vibrant ecosystem. Rewarding users for contributing their resources to the network can motivate active participation and sustained growth.
- Advanced Security Measures: Implementing sophisticated encryption mechanisms and algorithms can strengthen the security of the system. Ensuring robust data protection and access control mechanisms will instill confidence among users to store their data in the decentralized network.

In the future, our research lays the foundation for exploring additional applications of the decentralized storage system. One potential avenue is to investigate the integration of smart contracts to automate data access control and ensure secure data sharing between authorized parties. Additionally, we plan to explore the use of advanced encryption techniques to strengthen data privacy and confidentiality in the system. These potential enhancements will further reinforce the viability and effectiveness of the proposed solution.

VIII. CONCLUSION

By encrypting the data and distributing it among a large number of peers in the system, the suggested solution improves data security. To ensure the privacy of the user's data, the implemented system encrypts data using the AES 256-bit encryption algorithm. Afterwards, encrypted data is distributed and stored among network peers via the IPFS protocol. Our method not only addresses the privacy and security issues related to centralised cloud storage, but it also gives peers a platform to rent out idle storage and receive cryptocurrency in return, making the best use of the capacity that is available.

ACKNOWLEDGMENT

Akshar Mehta and Karan Parmar played pivotal roles in the development of this work, with Akshar leading the design and implementation of the smart contract and blockchain integration, and Karan focusing on frontend integration, UI/UX enhancements, and performance optimization. Nilesh Sahu contributed to the literature review, providing essential insights and supporting the project's foundation.

We wish to express our sincere gratitude to Dr. Sanjay U. Bokade, Principal, and Prof. S. P. Khachane, Head of Department of Computer Engineering at MCT's Rajiv Gandhi Institute of Technology, for providing us with the opportunity to work on our project, "Decentralised Storage System to Store Data using Blockchain Technology." This project would not have been possible without the guidance and encouragement of our project guide, Prof. S. P. Khachane, and the valuable

insights of our project expert, Prof. Bhushan Patil. We would also like to thank our colleagues and friends who helped us complete this project successfully.

REFERENCES

- [1] IPFS. "What Is IPFS? — IPFS Docs." IPFS Documentation — IPFS Docs, <https://docs.ipfs.tech/concepts/what-is-ipfs/>. Accessed 29 Oct. 2022. [1]
- [2] Karanth, Harsha, and Shuwam Rana. "Decentralized Storage. Introduction — by Harshakaranth — Coinmonks — Medium." Medium, Coinmonks, 21 Apr. 2022, <https://medium.com/coinmonks/decentralized-storage-701d53c4aa76>. [2]
- [3] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang and L. Sun, "A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications," in *IEEE Access*, vol. 6, pp. 27324-27335, 2018, doi: 10.1109/ACCESS.2018.2821705. [3]
- [4] Pham, Van-Duy, et al. "B-Box - A Decentralized Storage System Using IPFS, Attribute-Based Encryption, and Blockchain." 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, Oct. 2020. Crossref, doi:10.1109/rivf48685.2020.9140747. [4]
- [5] Shah, Meet, et al. "Decentralized Cloud Storage Using Blockchain." 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), IEEE, June 2020. Crossref, doi:10.1109/icoei48184.2020.9143004. [5]
- [6] Wang, Shangping, et al. "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems." *IEEE Access*, Institute of Electrical and Electronics Engineers (IEEE), 2018, pp. 38437–50. Crossref, doi:10.1109/access.2018.2851611. [6]