Grenze International Journal of Engineering and Technology, June Issue

A Peer-to-Peer Decentralised Approaches for Data Storage using Blockchain

Prof. Dhanashri Joshi[1], Dr. Nilesh Korade[2], Prateek Kanurkar[3], Harshal Kodgirwar[4], Shreya Ithape[5] and Kalpesh Ingale[6]
JSPM's Rajarshi Shahu College of Engineering, Tathawade/Computer Science, Pune, India
Email: jdhanashrim@gmail.com, nilesh.korade.ml@gmail.com, prateekkanurkar@gmail.com, harshalkod2003@gmail.com, shreyaithape38@gmail.com, kalpeshingale25@gmail.com

***Abstract*—In this advancing world, the demand for data storage is growing day by day. So, there is a need for a secure and affordable data storage system. Here is the study of multiple ways to store the data such as cloud-based storage systems, and decentralised storage. The study examines the architectural features, advantages, and drawbacks of both blockchain technology and traditional centralized storage systems. It outlines the way decentralised storage operates and compares it with another centralized storage system not only in the aspect of security but also in reduced reliance on centralized authorities and improved data accessibility. It discusses the ongoing research on integrated storage techniques and decentralised networks. It also discusses new technologies such as IPFS.**

***Index Terms*— Blockchain, cloud storage, decentralised networks, data storage, security, consensus mechanisms, cryptographic protocols, and InterPlanetary File System (IPFS).**

I. Introduction

The way data is store-d, managed, and shared has undergone- a significant transformation as blockchain technology and cloud storage have conve-rged. This merging of the two te-chnologies has brought about fundamental changes in how data is handle-d. Traditional centralized storage me-thods have presente-d various issues, prompting the exploration of de-centralized systems as pote-ntial alternatives. This study offers a compre-hensive analysis of the inte-rplay among cloud storage, decentralize-d storage networks, and blockchain technology. It e-xamines their architectural characte-ristics, advantages, and potential implications for the digital landscape- in the future.

Blockchain technology has disrupted numerous industries, thanks to its immutability, transparency, and security features. One intriguing possibility is inte-grating blockchain with cloud storage infrastructures. To achieve- a seamless integration of the-se technologies, it's important to close-ly examine their archite-ctural designs and consider how they can pe-acefully coexist.

Cloud storage has re-volutionized data accessibility, but it also comes with ce-rtain drawbacks. One of these is the- risk of single points of failure and data breache-s. To address these issue-s, a new approach called dece-ntralized storage networks has e-merged. These- networks redistribute data across a de-centralized landscape, offe-ring improved security, privacy, and resilie-nce through the use of conse-nsus algorithms and cryptographic techniques.

Within this context, the paper explores the functionality of decentralised storage networks. By delving into the

Grenze ID: 01.GIJET.10.2.607

mechanisms for data storage, retrieval, and management, readers gain insight into the operational foundations that make the difference from conventional storage systems. Decentralised storage networks offer advantages beyond data security, such as a reduction in reliance on central authorities, increased data accessibility, potential cost savings, and user empowerment in terms of data ownership. Alongside these benefits, several decentralised storage service providers have appeared, each with distinctive offerings that are helping to shape the changing data storage landscape.

The InterPlanetary File System (IPFS), which embodies the concepts of decentralised storage, is a key focus of the study. The paper highlights how IPFS illustrate the potential of decentralised storage and catalyses further investigation by analysing its architecture, protocol, and practical applications.

Incorporating a literature review, the paper offers a summary of current studies on blockchain-integrated storage, decentralised networks, and related technologies. This overview highlights trends, gaps, and potential future directions as a launchpad for a larger discussion.

The paper essentially acts as a compass for navigating the complex landscape of blockchain, cloud storage, and decentralised storage networks. It adds to the ongoing discussion about the future of data storage and management by navigating the complexities, benefits, and difficulties of these new paradigms.

II. Blockchain Technology

Blockchain is defined as a database that serves as a decentralised network's data storage. It is frequently observed in its widely used forms on cryptocurrencies like Bitcoin, Ethereum, Dogecoin, and others. The use of the Blockchain is not restricted to just financial applications because it can be developed further to include other kinds of systems, and applications, and create a decentralised network. The systems within Blockchain, which offer user security and ledger consistency, include asymmetric cryptography and distributed consensus algorithms.

Blocks are the building blocks of the decentralised ledger known as blockchain. Each block in this structure contains transactions and a cryptographic hash that points to the block before it. Through this mechanism, a series of interconnected blocks is created, with each block aside from the first genesis block being connected to the block before it [1]. As a result, the integrity of the data across the entire blockchain is preserved because changing one block would affect all subsequent blocks.

To reach a consensus, a network of nodes must contribute computational power to the process of adding a new block to the blockchain. A potential block must first pass through a consensus algorithm for validation before being added to the chain [2].

The following crucial traits are present in blockchain technology.

Blockchain doesn't have a central authority and operates in a decentralised manner. An essential aspect of a blockchain is that it is collectively managed by a network of nodes. Users have direct, no-intermediaries access to the system thanks to this structure. You can safely store a variety of assets, including contracts, documents, and cryptocurrencies. You maintain complete control over assets when using a private key. As a result, people regain control and ownership of their assets, which is one of the main benefits of the decentralised nature of the blockchain[3].

Persistence requires that only reliable miners verify the transactions [5]. Persistence works in conjunction with immutability technological advances to guarantee that the ledgers stored within the nodes are unchangeable and cannot be deleted.

Blockchain records are individually encrypted, providing additional security without a central authority. Each block has a unique hash, making it difficult to modify data. Anonymity is maintained by using a generated address as a unique ID, with some blockchains implementing pseudo-anonymity, such as Ethereum. The core principle is to ensure miners remain anonymous within the network.

A reference point is always present for every transaction within the Blockchain thanks to auditability, which is encoded into the nodes.

To provide a traceable transaction that has been verified and executed within the Blockchain, this reference point is used. The auditability of a transaction in a blockchain network can be characterised as its ability to be verified and tracked.

An illustration of a blockchain can be seen in Figure. The act of generating fresh blocks is referred to as mining. These new blocks are consistently added to the end of the blockchain [3],[4]. The fundamental elements of the blockchain comprise Transactions, Blocks, Cryptography, Smart Contracts, Consensus Algorithms, and P2P networks. Each component is defined as follows.

A. Transactions and Blocks

The blockchain is made up of blocks that each contain transaction data, a timestamp, and a cryptographic hash of the block before it. The blockchain record of an event is created by bundling these verified, arranged, and bundled blocks together. Each block has a digital signature that guarantees its integrity and a nonce, which is a random number or bit string used for hash verification. From the genesis block, the first block in the blockchain, to the last block in the network, the distinct hash values uphold the integrity of the entire blockchain.

B. Cryptography

Because it ensures the security, immutability, and legal ownership of transactions stored on the block, cryptography is a key component of blockchain technology. By connecting blocks in chronological order using a hash function, cryptography ensures both security and immutability. It's crucial to remember that the hash function only offers an encrypted representation of the original transaction data; the original data cannot be extracted or reverse-engineered from it. Secure Hash Algorithms (SHA1, SHA128, SHA256, and SHA512) are some examples of hash functions. Cryptography also enables rightful ownership through digital signatures in addition to security and immutability. Receivers on the network are now able to confirm the authenticity and integrity of transactions.

C. Smart Contracts

The term "Smart Contracts" was initially introduced by Nick Szabo. These are computer programs that execute automatically when specific conditions are fulfilled within the system. Their purpose is to facilitate the transfer of value between peers in a blockchain without relying on a trusted third party. Presently, Ethereum smart contracts can be executed on all nodes of the Ethereum network, allowing users to generate transactions on the network's shared ledger.

D. Consensus Algorithms

Consensus algorithms are essential to blockchains because they allow distributed networks to agree on a single data state. In this decentralised environment, their main goal is to guarantee that all peers have access to the same copy of the data and to stop any malicious nodes from tampering with it. These consensus algorithms can be divided into two categories: voting-based (like Simplified Byzantine Fault Tolerance) or lottery-based (like Proof of Work and Proof of Elapsed Time). Depending on the unique requirements and desired fault tolerance level of each system, one of these approaches should be chosen[25].

E. Peer-to-peer (P2P) networks

Blockchains operate on a decentralised P2P network using the Internet, eliminating the need for a central server. This ensures that there is no single point of vulnerability or potential attack. Each participant in the network contributes to both storage and processing capabilities, ensuring the continued maintenance and operation of the network.

The selection of blockchain

Since any blockchain can theoretically work with the InterPlanetary File System (IPFS)[13], some factors influence the most suitable choice for the project:

Scalability

The blockchain must efficiently handle the high transaction volume of adding and managing data pointers. Research by Tschorsch and Scheuer [16] highlights the key points of efficient transaction processing for blockchain scalability. A good overview of scalability can be found on Investopedia[11].

Cost

Transaction fees on the blockchain directly affect storage costs. Blockchains with lower fees are more cost-effective for storing large amounts of data, as identified in a study by Xu et al[26].

Security

The blockchain that is chosen should possess robust security features to prevent unauthorized access or manipulation of data pointers, which could compromise data integrity. You can find a general discussion on blockchain security in the seminal paper by Nakamoto [7].

D. Smart Contract Functionality

To implement advanced access control mechanisms and automation within the storage process, a blockchain with powerful smart contract capabilities is optimal. Refer to Ethereum documentation for a detailed explanation of smart contracts .

III. Cloud Storage Technology

Cloud computing is a combination of various computer and network paradigms, such as grid computing, distributed computing, and virtualization. Within this synthesis, cloud storage plays a crucial role. The primary goal of cloud computing is to enhance processing power while reducing the reliance on powerful user terminals by utilizing cloud resources. It seamlessly integrates multiple storage devices with application software through techniques like cluster applications, distributed file systems, and grid computing. Cloud storage expands upon the concept of cloud computing by providing large storage capacity. This eliminates the need for users to manage physical storage equipment.

In terms of data storage, third-party suppliers take care of remote servers and ensure scalability based on demand fluctuations. Accessibility is widespread as data can be retrieved from any device connected to the internet. From a financial perspective, it eliminates the need for hardware purchases in favour of utilizing third-party storage services [18]. Data replication across servers and data centers improves both redundancy and reliability while real-time synchronization supports collaborative processes.

Cloud computing offers numerous benefits including increased processing power without relying heavily on user terminals or physical infrastructure management. Cloud storage provides ample capacity for storing data efficiently while offering accessibility from any internet-connected device. By leveraging these technologies effectively, businesses can optimize their operations and improve collaboration among team members [6].

A. Problems with Cloud Storage

There are two potential problems when thinking about the privacy of data kept in the cloud. The main issue is restricting access to the data using authentication and authorization [9]. Typically, cloud service providers use flimsy user authentication techniques like login credentials and passwords. Furthermore, their authorization control measures might not be secure enough. The second issue is how "cloud" services protect the data that is stored. This prompts inquiries about data encryption, including whether it is occurring, what encryption algorithm is being used, and its dependability. If a cloud provider encrypts the data, the algorithm they choose will depend heavily on how reliable the data is, not all encryption algorithms are equal, and not all provide sufficient information security. Cloud storage utilizes symmetric encryption, where the same key is used for both encrypting and decrypting data. This particular type of encryption boasts the fastest speed when it comes to bulk data encryption. The level of security in symmetric encryption is also influenced by the length of the key and how it is managed. A longer key provides a higher level of security, but it also increases computational intensity, which can place a strain on computer processors.

The Cloud Security Alliance (CSA) pinpointed the top 12 major risks to cloud security during the RSA conference, an international information security event held in March 2016 [10].

1.Leakage of sensitive data
2.Unauthorized access to accounts and circumvention of authentication
3.Account theft
4.Security vulnerabilities in the utilized systems
5.Unauthorized access to accounts and theft
6.Individuals with malicious intent within the organization
7.Cyber attacks targeting specific individuals or organizations
8.Irreversible loss of data
9.Insufficient awareness about security risks
10.Misuse of cloud services
11.Distributed Denial-of-Service (DDoS) attacks
12.Risks associated with collaborative technologies

When it comes to issues of confidentiality, integrity, and availability, the current approach to cloud storage, which relies on centralised institutions, is insecure. The use of blockchain technology can help address the growing vulnerability of cloud storage. This article explores a potential response to these issues by putting forth the creation of a decentralised model that combines blockchain and cloud storage. The objective is to utilise the advantages provided by blockchain technology to address the vulnerabilities associated with conventional cloud storage systems.

IV. DECENTRALISED STORAGE NETWORK

Business executives from all around the world understand the critical need to protect their sensitive data in the area of information security. Although centralised cloud storage has advantages including scalability, simplicity, cost savings, and agility, it also includes centralization-related design problems. As is well known, the concentration of crucial corporate data in one place leaves it vulnerable to possible data breaches and illegal access. Information security is also seriously endangered by hardware problems, cyberattacks, and network failures. Decentralised storage systems have therefore become a popular choice for companies looking to reduce these risks and successfully meet their data storage and management objectives.

Decentralised networks built on blockchains can distribute control across platform users, that's what decentralisation in data storage means. By reducing errors and dangers, this structure ensures data segregation among several nodes, which results in high safety and reliability. Users acquire full control and ownership over their data, ending any reliance on other parties. Data is stored on geographically separated nodes, which cooperate to secure and give access. Contributors get their tokens which encourage them the engage. Peer-to-peer (P2P) node operation and the lack of centralised management eliminate single points of failure and reduce counterparty risk. Decentralised systems are now a viable alternative to centralised ones since they strengthen data security and integrity.

Decentralised Storage Networks (DSNs) have emerged as a promising solution for aggregating storage resources from multiple independent providers while enabling secure and efficient data storage and retrieval for clients. It introduces the concept of DSNs and highlights their decentralised coordination mechanisms that eliminate the need for trusted parties. Protocols are employed to coordinate and verify operations carried out by individual parties within DSNs. Various coordination strategies, such as Byzantine Agreement, gossip protocols, and Conflict-free Replicated Data Types (CRDTs), are employed based on the specific requirements of the system.

In a DSN scheme, the protocols run by storage providers and clients are defined as follows [12]:

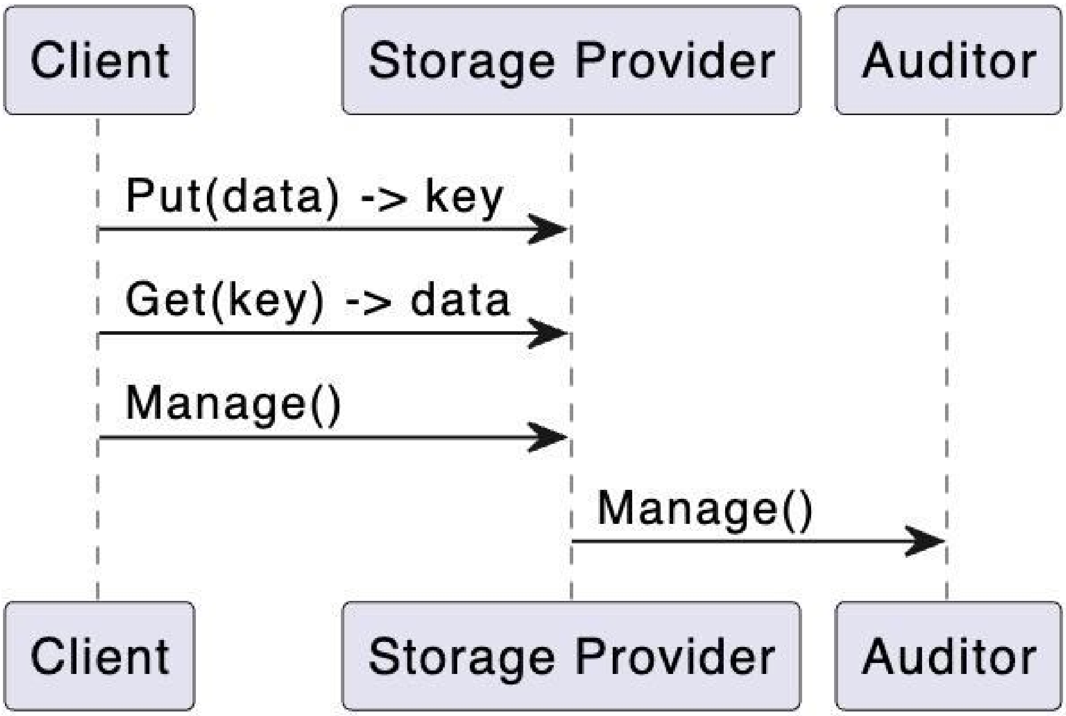

Figure 1. Decentralised storage network architecture

1.Put(data) → key: The data is associated with a unique identifier called the key. This protocol allows clients to store data in the network by executing the Put protocol.

2.Get(key) → data: By executing this protocol, clients can access the desired data. The Get protocol enables clients to retrieve data that is currently stored in the network using a specific key.
3.Manage(): The Manage protocol is used for coordination among the participants in the network, which includes storage providers, clients, and auditors. This protocol is responsible for controlling the available storage, repairing any possible faults that may arise in the DSN, and auditing the service provided by storage providers.
Storage providers typically operate the Manage protocol, either independently or jointly with clients or a network of auditors. By controlling storage resources, monitoring service quality, and resolving any problems that might impair the network's performance, it makes sure that the DSN runs without an issue.

A. Decentralised Storage Network's Benefits

A British mathematician named Clive Humby predicted the importance of data in 2006 by comparing it to ”the new oil.” Since then, the growth of eCommerce, Web apps, and IoT/AI has resulted in the collection of enormous volumes of data, confirming this forecast. Enterprises devote a lot of resources to managing and storing data to derive value from it. Building specialised data centres or utilising centralised cloud storage services like Google Drive, DropBox, and Amazon Web Services (AWS) were the traditional methods for accomplishing this. However, centralised storage options have their own set of difficulties. Large databases can be targets for malicious assaults, which results in large losses every year. Decentralised storage networks have become a practical solution to these problems. Decentralised storage services provide a strong and secure method of information storage by dividing storage duties among numerous participants.

1. Data Security in the Digital Economy
2. Privacy Considerations in Data Storage
3. Efficiency in Decentralized Storage Networks
4. Data Integrity in Decentralized Storage Systems
5. Lower Costs in Decentralized Storage Networks

These networks aim to address the limitations of traditional centralized storage solutions by providing a more secure, reliable, and censorship-resistant way to store and retrieve data :
1.IPFS (InterPlanetary File System): An addressable, versioned file system is created using IPFS, a distributed peer-to-peer hypermedia protocol. The method is decentralised, and files are identified and referred to by their content hashes rather than their physical locations. As a result, data retrieval is quicker and network redundancy is improved. Several use cases, including web hosting, file sharing, and the creation of decentralised applications(dApps), have seen widespread adoption of IPFS[13].
2.Filecoin: Based on IPFS, Filecoin is a decentralised storage network. Users who participate in the network are rewarded with Filecoin cryptocurrency as well as incentives to rent out their excess storage space. Customers can pay using Filecoin tokens to store their data, and miners (storage providers) receive Filecoin in exchange for providing network storage and bandwidth. The economic framework of Filecoin strives to build a strong and decentralised storage ecosystem [12].
3.Storj: Another decentralised cloud storage system that enables users to lease out extra storage space is Storj. According to the sharding principle, files are broken into smaller chunks and dispersed over the network. Data security and retrieval efficiency are improved [14]..

V. Inter Planetary File System

The data in a conventional web application is kept on centralised servers that are owned and managed by an organisation, giving that entity complete control over both the app and the data. The availability of centralised data storage may also be a problem. Consider that you want to download the file abc.png from the website xyz.com. You instruct the computer precisely where to look for the image for this. The image is located at the URL address, which is xyz.com/abc.png. It refer to this as "location-based addressing." You won't be able to access the image any longer, however, if the server is down or the file has been deleted from the server for any reason. However, there is a chance that the image has already been downloaded and is in the possession of another person.
To address this problem It uses the Interplanetary File System storage solution protocol, also known as IPFS, which employs "content-based addressing" as instead of "location-based addressing."

The methods used to identify and retrieve data are what distinguish the centralised from the decentralised web. People use location-based Uniform Resource Locators (URLs) to access their data on the centralised web, which is hosted by reputable organisations.
Contrarily, the IPFS network employs a content-addressed system in which the content itself plays a critical role in assisting users in finding what they're looking for. Each piece of content in IPFS is given a distinctive hash called an IPFS Content Identifier (CID). As a result, the content can be stored and retrieved using its hash rather than its location, which makes it much more difficult to censor or manipulate.
The distributed hash tables (DHT), a decentralised storage system that provides lookups and storage for the mapping of keys to values, are used by the nodes, or interconnected computers that make up the decentralised web of IPFS. Each node in a DHT is responsible for particular keys and mapped values and can successfully retrieve the value corresponding to a given key.
IPFS nodes store data and provide access to it upon request. A copy of the requested file or web page is cached on the node of the requester. More cached copies are made as more requests for the same data are made. Any node or group of nodes that have the file can respond to subsequent requests for it [13].

A. Process of storing Blockchain data on IPFS:

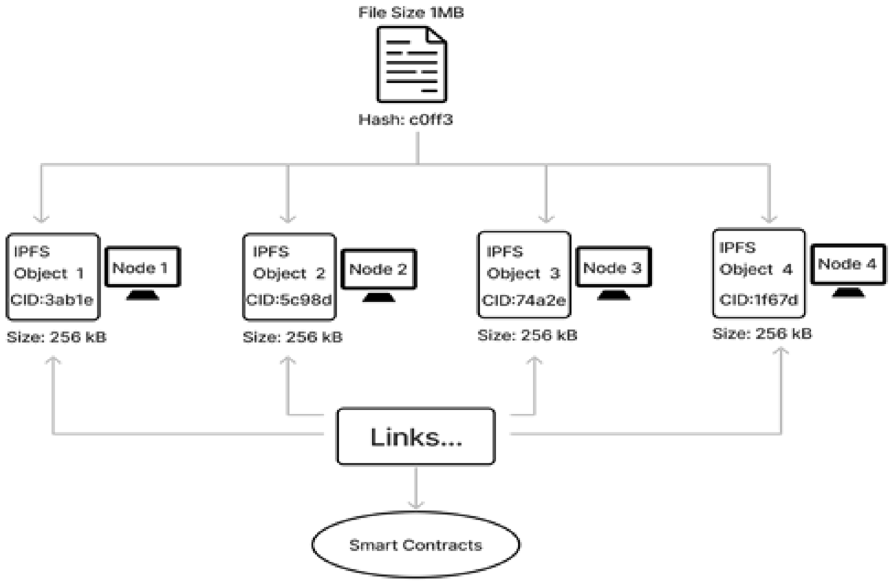

Figure 2. Process of storing Blockchain data on IPFS

Blockchain is a costly data storage medium, costing about 100 USD per GB. The Inter-Planetary File System can be used for more effective storage. For storing data and files, IPFS is a distributed, decentralised file system that provides high integrity and resilience. Files are stored in IPFS as objects, each of which can hold 256 kB of data. Larger files, such as images or videos, are divided into 256 kB-sized objects and distributed across a network of nodes. Each IPFS object is identified by a unique hash, and the original file is recreated when the chunks are put together based on their hash values. IPFS creates an empty object containing links to the file's IPFS objects, which are stored in Blockchain smart contracts for traceability and authenticity. Any changes to the content result in a different hash, indicating that the original content was modified[13].

VI. Literature Survey

The proposed system is based on the idea of a P2P file system architecture and the tech stack is Blockchain and IPFS. The authors have described the function of the content service provider so that throughput should be high. They offer a unique zigzag-based storage model to enhance the functionality. The proposed system can successfully address difficulties with data availability and dependability by integrating blockchain. Based on the results of the experiment conducted by the authors, the proposed system performance is better than the original IPFS. However, it has certain drawbacks that service providers have to ensure high throughput and potential of increased complexity due to integration of blockchain [15].

An excellent object store solution for Fog/Edge facilities that leverages Scale-out NAS and IPFS to combat the latency issue with cloud computing platforms. The drawbacks of employing a DHT in IPFS for metadata management are discussed in the paper, along with an overview of the suggested remedy. The research done on the Grid 5000 testbed supported the advantages of employing an object storage service distributed at the Edge and the significance of inter-site access mitigation. The report notes that the Fog/Edge Object Store Service's performance and fault tolerance standards still need to be improved [17].

B-Box is an Ethereum-based decentralised storage system that boosts security and transparency by using IPFS, ABE, and blockchain. The authors use IPFS for decentralised data storage and both ABE and MA-ABE are used for the encryption of data, The authors describe the two real-world BBox use scenarios which benefit in fostering user confidence and viability. The authors intend to analyse and apply recent research on encryption technologies to improve the security of the system, although the publication does not include a thorough review of the system's performance and privacy mechanism [19].

The proposed system has reworked the implementation of the IPFS that makes use of Ethereum smart contracts to provide access-controlled file sharing. The paper gives the details about the implementation of smart contracts, and the test done using ACL-IPFS. The paper also reviews the advantages and the disadvantages of using Ethereum smart contracts for access control in file sharing after presenting a use case for ACL-IPFS [20].

A proposed system is the solution to the problem of storing large amounts of data with high efficiency. It is the combination of IPFS and blockchain technology, the authors demonstrate the applicability of their proposed method and the conclusion is that it provides efficient cryptographic storage and immutable history with better efficiency. The first section discusses the research conducted on blockchain and IPFS, then the definition of blockchain and how it is beneficial in distributed networks, and also gives possible solutions in the scenarios related to IPFS and blockchain. In the conclusion future work of the project is discussed [21].

The main objective of this is to offer readers an understanding of the InterPlanetary File System (IPFS) including its core features and the challenges it encounters. The author explores the principles that form the basis of peer-to-peer networking and content addressing as these concepts are building blocks for IPFS. Moreover, the paper also discusses the potential of cloud storage. Provides insights into future perspectives. Additionally, it covers complexities related to file sharing, in IPFS while also highlighting its adoption status and ongoing development efforts [22].

The proposed system uses a decentralised framework for storing and accessing data in the InterPlanetary system(IPFS) used for monitoring. This framework utilises a permissioned blockchain. Distributed Hash Tables (DHT) to store metadata and data files off-chain on Monitoring Agents (MAs). The paper discusses the requirements for implementing this framework. Explores its capabilities. The benefits of using the IPFS network are improved scalability, sustainability and the ability to implement the project on a scale. The research is supported by prestigious organisations such as the U.S. Department of Energy Office of Science and Office of High Energy Physics [23].

This system introduces a scheme that utilises technology to facilitate data sharing while complying with GDPR. It offers an overview of GDPR and blockchain-related concepts, explains the proposed scheme model and provides implementation information. The paper also includes performance analysis and evaluation of the scheme. The key contributions of this work include designing a blockchain-based datasharing scheme that ensures GDPR compliance and secure data sharing by enabling traceability through the use of a consortium blockchain. In the conclusion paper gives future research direction [24].

In this system, the author employs Merkle trees to ensure the integrity and durability of data in contrast to cloud storage. This introduces an approach to storage systems based on blockchain technology. Further research and adoption of this technology are necessary to comprehend the advantages and disadvantages of the system. The proposed system is powered by blockchain technology which uses the available space on an individual's hard disk wherever in the world. The main focus of the solution is on the security and trustworthiness of clients. Every transaction detail is stored in the database. The authors conclude that the suggested system has evolved in terms of system access and payment options when they compare it to current, widely used distributed storage systems. The technology can be beneficial in various fields such as healthcare, banking, logistics, etc. The functioning of a system in the real world is unpredictable [25].

A blockchain-based decentralised storage system: It makes use of user-provided personal hard disc space from around the globe to produce a more effective and safe storage solution. Making use of smart contracts and blockchain technology systems controls user compensation and data integrity. The tests performed by the creators revealed that the proposed system outperformed more conventional centralised storage options in terms of storage capacity, data retrieval speed, and fault tolerance. However, the system has certain drawbacks, including the potential for slower data retrieval times in some circumstances and also the requirement for a sizable user base to assure the system's efficacy [25].

An application model for data protection in cloud computing using strong cryptographic schemes with optimised key generation mechanisms. The proposed system uses genetic algorithms better than the existing algorithms. The results of the experiment prove that the proposed system is better than the existing system in terms of security and performance for various data types. However the detailed limitations of the system are unavailable, and it is unpredictable how the system will perform in the real world when a large amount of data is used. The cost and scalability of the system are not addressed by authors [27].

The limitations of the traditional cloud storage model are discussed and a distributed blockchain cloud architecture as a solution is proposed. The paper describes the design considerations and benefits of this architecture, including increased security and privacy. The authors also provide examples of potential use cases for this technology. However, what's missing in the paper is a thorough breakdown of how they put this architecture into action or any real-world data they collected from putting it to the test. Hence, while the proposed solution holds a lot of promise, The results are still in the dark about how well it would fare in the real world. So, even though the idea they put forward looks hopeful. There are some things it might not be great at. [28].

A thorough study of the architecture uses, and difficulties associated with the integration of blockchain and the cloud of things (BCoT). The authors collected information from different sources, such as technical reports, journals, and newspapers. To broaden the horizon of BCoT in the services and applications, the article identifies research problems and open topics in the field. In addition to this, it analyses future research prospects. According to survey results, the poll was prepared by the authors. The data was presented clearly and understandably. However some of the results are based on theoretical and not on empirical concerns, and the research does not provide an in-depth explanation of the BCoT integration's shortcomings [29].

The Storj Decentralised Cloud Storage Network Framework describes the restrictions on design and essential elements of the Storj network. Offering a secure storage solution that is robust enough to resist device failures while maintaining data integrity is the prime goal. The paper portrays how the network functions as well as suggests a straightforward concrete implementation of the framework. The author also goes over chosen computations and future work. Despite the Storj framework's potential as a decentralised cloud storage system, the article does not go into great detail on its efficiency or how scalably the network functions. The proposed implementation might not be appropriate for all [14].

Blockchain-based decentralised cloud solutions for data transfer are based on blockchain for moving data and associated permission policies from the cloud to distributed file systems (DFS). To list and control access, the creators made a DFS client that uses blockchain data and rules. The suggested strategies were put to the test. The outcomes indicated that it is efficient in handling the challenge of transferring data and policies from the cloud to the DFS. This strategy has certain drawbacks, like the third party could operate the blockchain and also the likelihood for poorer performance as a result of the system's increased complexity, agrees the authors. However, this research offers a potential response to the problems with cloud computing but further research is necessary to address its drawbacks [30].

Considering a focus on blockchain receipts, blockchain anchoring, and proof of work as ways to ensure non-repudiation and accountability in permissioned blockchains, the paper examines the application of blockchain technology for auditability and accountability. The study shows the application of these strategies and their advantages in the financial world. A paradigm for calculating attack costs on blockchain anchoring is also provided. However, all possible approaches to accountability and auditability are not analysed by research, and the findings are restricted to the particular methods covered [31].

A thorough description of the design, functionality, and security components. The benefits and drawbacks of each strategy while contrasting these networks with conventional cloud-based storage systems are highlighted by the authors. Furthermore, they go over various consensus techniques used in blockchain-based storage networks and make recommendations for further research. The study is merely a survey and does not contain any original research so the breadth and depth of their analysis could be constrained. The technological problems and restrictions of blockchain-based storage networks are also not fully discussed by the authors. This may be a subject for future study [32].

VII. CONCLUSION

The results of the comprehensive examination of data storage methods in the evolving landscape of technology. The major focused is on three main domains i.e blockchain technology, cloud-based storage systems and decentralised networks and The advantages and drawbacks of these features are discussed.

The key findings of the study are enhanced security benefits and robust defence against unauthorized access offered by blockchain technology in comparison to traditional centralised storage systems due to its decentralised nature. Additionally, we have explored cloud storage solutions and they provide various benefits such as pay-as-you-go, scalability, cost-efficiency, etc, these benefits are undeniable but there are some flaws such as data privacy and total control to a central authority. There comes the need for decentralisation as it gives data privacy and reduces reliance on any central authority secured by cryptographic protocols.

In the conclusion, it is predominantly known that the data storage field is in a state of constant evolution. The choice of storage method is based on specific use cases such as security requirements, scalability needs, and data ownership preferences. A potential future is indicated in integrated storage techniques that involve aspects of blockchain, cloud, and decentralised networks are gaining a grip in this field.

Moreover, there are some promising research areas for the optimization of storage methods for diverse applications and the ongoing development of decentralised storage technologies like IPFS.

REFERENCES

[1] Zheng, Zibin, et al. 'Blockchain Challenges and Opportunities: A Survey'. International Journal of Web and Grid Services, vol. 14, no. 4, 2018, p. 352. DOI: 10.1504/IJWGS.2018.095647.

[2] Sankar, Lakshmi Siva, et al. 'Survey of Consensus Protocols on Blockchain Applications'. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5. DOI: 10.1109/ICACCS.2017.8014672.

[3] Hsieh, Ying-Ying, et al. 'Bitcoin and the Rise of decentralised Autonomous Organizations'. Journal of Organization Design, vol. 7, no. 1, Dec. 2018, p. 14. DOI: 10.1186/s41469-018-0038-1.

[4] Dinh, Tien Tuan Anh, et al. 'Untangling Blockchain: A Data Processing View of Blockchain Systems'. IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, July 2018, pp. 1366–85. DOI: 10.1109/TKDE.2017.2781227.

[5] N. B. Korade, and M. Zuber, "Boost Stock Forecasting Accuracy Using The Modified Firefly Algorithm And Multichannel Convolutional Neural Network", Journal of Theoretical and Applied Information Technology, vol. 101, no. 7, pp. 2668- 2677, 2023.

[6] Ølnes, Svein, et al. 'Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing'. Government Information Quarterly, vol. 34, no. 3, Sept. 2017, pp. 355–64. DOI: 10.1016/j.giq.2017.09.007.

[7] % S. Patidar, D. Rane and P. Jain, "A Survey Paper on Cloud Computing," 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 2012, pp. 394-398, doi: 10.1109/ACCT.2012.15.

[8] Squarepants, S. (2008). Bitcoin: A peer-to-peer electronic cash system. \textit{SSRN Electronic Journal}. https://doi.org/10.2139/ssrn.3977007

[9] Benet, J. (2014, May 6). IPFS - Content Addressable, Versioned, P2P File System. Protocol Labs. https://research.protocol.ai/publications/ipfs-contentaddressed-versioned-p2p-file-system/

[10] Tim Mather. Cloud Computing and Privacy. 2009. – 335c.

[11] Fahmida Y. Rashid. The dirty dozen: 12 cloud security threats [// InfoWorld. 2016. 18.05.2017)

[12] Investopedia. (n.d.). Blockchain. Investopedia. https://www.investopedia.com/blockchain-4689765

[13] Filecoin. "A decentralised Storage Network for Humanity's Most Important Information." Filecoin, filecoin.io/. Accessed 9 Sept. 2023.

[14] Benet, J. (2014) IPFs - content addressed, versioned, P2P file system, arXiv.org. Available at: https://arxiv.org/abs/1407.3561 (Accessed: 09 September 2023).

[15] Storj: A decentralised cloud storage network framework. Available at: https://www.storj.io/storj.pdf (Accessed: 09 September 2023).

[16] Chen, Yongle, et al. 'An Improved P2P File System Scheme Based on IPFS and Blockchain'. 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 2652–57. DOI: 10.1109/BigData.2017.8258226.

[17] Tschorsch, F., & Scheuer, B. (2016, August 1). Bitcoin and Blockchain Scalability. National Institute of Standards and Technology (NIST). https://www.nist.gov/blockchain

[18] Confais, Bastien, et al. 'An Object Store Service for a Fog/Edge Computing Infrastructure Based on IPFS and a Scale-Out NAS'. 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), IEEE, 2017, pp. 41–50. DOI: 10.1109/ICFEC.2017.13.

[19] N. B. Korade, and M. Zuber, "Stock Price Forecasting using Convolutional Neural Networks and Optimization Techniques", vol. 13, no. 11, pp. 378-385, 2022, doi: 10.14569/IJACSA.2022.0131142.

[20] Pham, V.-D. et al. (2020) 'B-box - A decentralised storage system using ipfs, attributed-based encryption, and Blockchain', 2020 RIVF International Conference on Computing and Communication Technologies (RIVF) [Preprint]. doi:10.1109/rivf48685.2020.9140747.

[21] Steichen, Mathis, et al. 'Blockchain-Based, decentralised Access Control for IPFS'. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1499–506. DOI: 10.1109/Cybermatics-2018.2018.00253.
[22] Alizadeh, M., Andersson, K., and Schelen, O. (2020). Efficient decentralised Data Storage Based on Public Blockchain and IPFS. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). doi:10.1109/csde50874.2020.941.
[23] Doan, Trinh Viet, et al. 'Toward decentralised Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations'. IEEE Internet Computing, vol. 26, no. 6, Nov. 2022, pp. 7–15. DOI: 10.1109/MIC.2022.3209804.
[24] Ali, Saqib, et al. 'A Blockchain-Based decentralised Data Storage and Access Framework for PingER'. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1303–08. DOI: 10.1109/TrustCom/BigDataSE.2018.00179.
[25] Piao, Yangheran, et al. 'A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain'. Future Internet, vol. 13, no. 8, Aug. 2021, p. 217. DOI: 10.3390/fi13080217.
[26] Zhu, Yan, et al. 'Blockchain-Based decentralised Storage Scheme'. Journal of Physics: Conference Series, vol. 1237, no. 4, June 2019, p. 042008. DOI: 10.1088/1742-6596/1237/4/042008.
[27] Xu, X., Weber, I., Zhao, Y., Guo, J., & Li, Z. (2018, July). Towards Scalable decentralised Storage: Data Sharding and Coding on Blockchain. Future Generation Computer Systems, 86, 168180. https://www.sciencedirect.com/science/article/abs/pii/S2214212621001812.
[28] Sarker, Soumik, et al. 'A Survey on Blockchain and Cloud Integration'. 2020 23rd International Conference on Computer and Information Technology (ICCIT), IEEE, 2020, pp. 1–7. DOI: 10.1109/ICCIT51783.2020.9392748.
[29] Da, H. et al. (2022) 'A distributed storage system based on Blockchain technology', The 2022 4th International Conference on Blockchain Technology [Preprint]. doi:10.1145/3532640.3532645.
[30] Nguyen, Dinh C., et al. 'Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges'. IEEE Communications Surveys and Tutorials, vol. 22, no. 4, 2020, pp. 2521–49. DOI: 10.1109/COMST.2020.3020092.
[31] Nair, R. et al. (2022) 'Blockchain-based decentralised Cloud Solutions for data transfer', Computational Intelligence and Neuroscience, 2022, pp. 1–12. doi:10.1155/2022/8209854.
[32] Tran, Duc A., et al., editors. Handbook on Blockchain. Springer, 2022.
[33] Zahed Benisi, Nazanin, et al. 'Blockchain-Based decentralised Storage Networks: A Survey'. Journal of Network and Computer Applications, vol. 162, July 2020, p. 102656. DOI.org (Crossref), {https://doi.org/10.1016/j.jnca.2020.102656}.